NEU!

www.tecChannel.de

tecCHANNEL SPECIAL

PDF-KOMPENDIUM FÜR IT-PROFIS

€ 4.90

Grundlagen der IT-Sicherheit

14 tecCHANNEL-Artikel zumThema in einem eBook

Security im Überblick (Teil 1)

› Die globale Vernetzung von Computern rückt zunehmend Fragen der Rechner- und Netzsicherheit ins Blickfeld. Unsere Artikelserie bietet Ihnen einen Überblick über alle Security-Aspekte. Der erste Teil führt in das Feld der Kryptologie ein.

› VON AXEL SIKORA

Mit der steigenden Verbreitung computer- und netzwerkgestützter Anwendungen gewinnt die Frage der Computer- und Netzwerksicherheit immer größere Bedeutung. Dies ist vor allem auf fünf Aspekte zurückzuführen:

- › Die Nutzung von öffentlichen Netzwerken durch Laien führt dazu, dass zahlreiche unzureichend konfigurierte und damit relativ ungeschützte Systeme im Netz eine breite Angriffsfläche bieten.
- › Automatisierte, im Internet verbreitete Werkzeuge - oft sogar mit grafischen Oberflächen - machen die Vorbereitung und Ausführung eines Angriffs sehr einfach. Das Hacken im Netz entwickelt sich zunehmend von einer Spezialistendisziplin zum Kinderspiel.
- › Auf Grund immer kürzerer Entwicklungszyklen (Stichwort: Time to Market) weisen alle Software-Lösungen mehr oder weniger gravierende Sicherheitslücken auf. Ein Nachführen von Bugfixes und Patches fällt wegen der Masse speziell Netzwerk-Administratoren zunehmend schwerer.
- › Definition, Implementierung und Einsatz von Sicherheitskonzepten gestalten sich in der Regel sehr komplex. Statt definierte, maßgeschneiderte Lösungen aufzusetzen, begnügen sich viele Anwender mit dem Einsatz proprietärer und isolierter Produkte. Ein trügerisches Gefühl von Sicherheit ist die Folge.
- › Der mobile Einsatz von Rechnern nimmt stetig zu. Besonders drahtlose Übertragungstechniken, aber auch der wachsende Einsatz von Remote Access (Dial-In/VPN) schaffen neue Herausforderungen an Sicherheitsarchitekturen.

› Safety und Security

Im Zusammenhang mit Rechnern und Netzen lässt sich Sicherheit als Nichtvorhandensein von Gefahren oder wirksamer Schutz vor Risiken beschreiben. Damit handelt es sich um eine nur subjektiv wahrnehmbare Größe, die man weder direkt sehen noch messen kann.

Die englische Sprache bietet die im Deutschen leider fehlende Unterscheidung zwischen *safety* und *security*, die zwei verschiedene Aspekte von Sicherheit näher eingrenzt. Safety bezieht sich auf die Zuverlässigkeit eines Systems, speziell in Bezug auf dessen Ablauf- und Ausfallsicherheit. Security bezeichnet dagegen den Schutz eines Systems vor beabsichtigten Angriffen. Die beiden Begriffe sind nicht völlig unabhängig voneinander: Safety schließt auch Security mit ein.

Unsere Artikelserie zum Thema Sicherheit konzentriert sich auf den Aspekt der Security und beschäftigt sich dabei mit folgenden Unterthemen:

- › Vertraulichkeit (confidentiality, privacy): Sicherheit gegen Angriffe durch unerlaubtes Abhören
- › Integrität (integrity): Schutz gegen die (meist partielle) Veränderung von Informationen. In Netzwerken kann die Integrität sowohl auf die Inhalte von Datenpaketen als auch auf deren Steuerinformationen und hierbei insbesondere

auf die Adressierung beziehen.

- Authentifizierung (authentication, auch non-repudiation): Überprüfung, ob ein Sender wirklich derjenige ist, der er zu sein vorgibt.
- Verfügbarkeit (availability) und Zugang (access): Informationen sind nur dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

Der hier vorliegende erste Teil der Serie beschäftigt sich mit der Sicherstellung der Vertraulichkeit: Wir werfen einen näheren Blick auf Grundlagen und Verfahren der Kryptographie.

Grundlagen: Security

› Kryptographie

Das Wort Kryptographie ist aus den griechischen Wörtern krypto (versteckt, geheim) und graph (Schrift, Wort) entlehnt. Damit bedeutet Kryptographie im Ursprung so viel wie Geheimschrift.

Kryptographie behandelt zum einen die Verschlüsselung (encryption), also die Transformation einer verständlichen Informationsdarstellung (Klartext, plain text, clear text) in eine nicht verständliche Darstellung (verschlüsselter Text, Geheimtext, cipher text). Diese muss in einer Weise erfolgen, dass die angewandte Transformation im Rahmen einer Entschlüsselung (decryption) von Befugten wieder eindeutig rückgängig gemacht werden kann.

Vor Dritten wird also nicht die Existenz der Information versteckt, sondern nur deren Bedeutung. Dieser Aspekt der Vertraulichkeit wird auch als Konzelation bezeichnet. Mit dem Verbergen von Informationen beschäftigt sich eine spezielle Variante der Kryptographie, die Steganographie (steganos, Griech: bedeckt).

Im erweiterten Sinne zählen zur Kryptographie auch Aufgaben der Integritätsprüfung und Authentifizierung. Oft basieren entsprechende Funktionen auf eingeschränkten kryptographischen Verfahren, bei denen die Verschlüsselung nicht unbedingt rückgängig gemacht werden muss. Es gilt lediglich sicherzustellen, dass zwei unterschiedliche Eingaben nur mit einer sehr geringen Wahrscheinlichkeit das gleiche Ergebnis liefern.

› Transposition vs. Substitution

In der Kryptographie unterscheidet man zwei grundsätzliche Schlüsselverfahren. Die Transposition ändert die Anordnung der Zeichen in der Folge, lässt das Auftreten der Zeichen jedoch unverändert. Dies kann man beispielsweise dadurch erreichen, dass man jeweils zwei aufeinander folgende Buchstaben austauscht: aus *Kryptographie* wird dann *Rkpyotrgpaihe*.

Als Scrambling ("Verwürfeln") wird Transposition auch bei vielen drahtlosen Übertragungstechniken eingesetzt. Dort entschärft sie den Einfluss von Büschelfehlern (burst errors), die mehrere aufeinander folgende Zeichen in der Übertragung stören. Nach dem "Descrambeln" folgen die gestörten Bereiche nicht mehr unmittelbar aufeinander. Sie verteilen sich über einen größeren Bereich, so dass Fehlererkennungs- und Korrekturmechanismen besser greifen.

Das zweite grundsätzliche Kryptverfahren, die Substitution, ersetzt Zeichen des Klartextes im Geheimtext durch andere Zeichen. Ein einfaches Beispiel dafür ist die vom

gleichnamigen römischen Kaiser gern verwendete Cäsar-Addition. Sie ersetzt jeden Buchstaben des Klartextes durch den, der im Alphabet drei Plätze weiter hinten steht. So wird aus *Kryptographie* der Chiffretext *Nucswrjudsklh*.

› Symmetrische Substitution

Die symmetrische Substitution verdankt ihren Namen der Tatsache, dass Sender und Empfänger in Besitz des gleichen Schlüssels sein müssen, um vertraulich miteinander zu kommunizieren. Außer den beiden Kommunikationspartnern darf niemand den Schlüssel kennen (Secret-Key-Verfahren).

Symmetrische Verfahren erreichen auch bei der Implementierung als Software akzeptable Verschlüsselungsraten. Sie eignen sich deshalb besonders gut zur Verschlüsselung großer Datenmengen. Der große Nachteil: Um die Nachrichten verwerten zu können, muss der Empfänger in den Besitz des verwendeten Schlüssels gelangen. Die Übertragung des Schlüssels stellt einen Schwachpunkt dar, an dem ein Angreifer ansetzen kann.

Zudem benötigen je zwei miteinander kommunizierende Partner einen exklusiven, geheimen Schlüssel. Die Anzahl der benötigten Schlüssel m hängt quadratisch von der Anzahl n der kommunizierenden Partner ab (m = 0,5 * n * (n-1)).

› Symmetrische Substitutionsverfahren

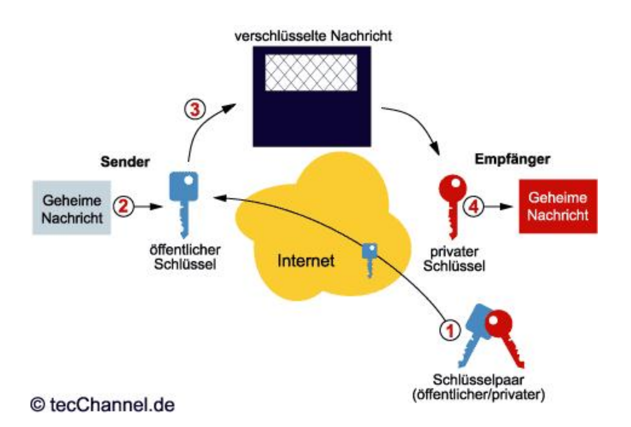
Symmetrische Verfahren lassen sich in Zeichen-, Block- und Stromchiffren klassifizieren. Die zeichenorientierte Substitution ermittelt jedes Zeichen des Geheimtexts aus dem entsprechenden Zeichen des Klartextes unter Zuhilfenahme des Schlüssels. Das einfachste Beispiel dafür ist die bereits erwähnte Cäsar-Chiffrierung.

Stromchiffrierungen verschlüsseln den Klartext Byte-weise über eine XOR-Operation. Dazu erzeugen sie in Abhängigkeit vom gewählten Schlüssel eine sich zyklisch verändernde Byte-Folge, die mit dem Klartext verknüpft wird. Durch ein erneutes XOR kann der Empfänger den Klartext rekonstruieren. Das macht Stromverschlüsselung sehr schnell, zudem lässt sie sich ideal in Software implementieren. Das bekannteste Beispiel einer Stromchiffrierung ist der RC4-Algorithmus.

Die blockorientierte Substitution fasst Bitgruppen des Klartexts in Blöcken zusammen und transponiert diese mittels in der Regel mehrstufiger Verfahren anhand des Schlüssels über gleich bleibende Operationen in den Geheimtext. Die bekannteste Blockchiffrierung ist DES.

› Asymmetrische Substitution

Eine elegante Alternative zu den symmetrischen Kryptverfahren bietet die so genannte asymmetrische Verschlüsselung. Sie verwendet zwei komplementäre Schlüssel, die so ausgewählt werden, dass mit dem einen Key chiffrierte Nachrichten nur mit dem zweiten Key wieder dechiffriert werden können. Einen der beiden Schlüssel kann man also gefahrlos öffentlich bekannt geben, weswegen man diese Vorgehensweise auch als Public-Key-Verfahren bezeichnet.



Public-Key-Verfahren: Mit dem öffentlichen Schlüssel des Empfängers lassen sich Nachrichten so verschlüsseln, dass sie auch nur mit dessen privatem Schlüssel wieder zu entziffern sind.

Den privaten zweiten Schlüssel nennt man Private Key, den frei zugänglichen Public Key. Eine mit dem öffentlichen Schlüssel chiffrierte Nachricht kann nur mit dem privaten Schlüssel dechiffriert werden. Anders herum gilt auch, dass sich eine mit dem Private Key chiffrierte Nachricht nur mit dem öffentlichen Schlüssel dechiffrieren lässt.

Public-Key-Chiffrierungen basieren auf einem mathematischen Bezug zwischen den verwendeten privaten und öffentlichen Schlüsseln. Dieser muss so komplex sein, dass Außenstehende nicht aus der Kenntnis des Public Key auf den passenden Private Key schließen können.

› Vorteile von Public-Key-Verfahren

Die Verwendung von Public Keys bringt vor allem den Vorteil, dass jeder Kommunikationspartner nur einen Schlüssel (seinen Private Key) benötigt. Als zweiten Schlüssel kann er den Public Key der Gegenstelle einsetzen, der ja öffentlich bekannt ist. Das entschärft das Skalierungsproblem der symmetrischen Verschlüsselungsverfahren wesentlich.

Als Nachteil handelt man sich andererseits bei den Public-Key-Verschlüsselungen eine hohe Komplexität der durchzuführenden Operationen ein. Die meisten asymmetrischen Substitutionsverfahren beruhen auf mathematischen Funktionen wie der Multiplikation oder der Exponentialfunktion. Die Multiplikation zweier Zahlen stellt eine einfache Operation dar, während der umgekehrte Vorgang, also die Faktorzerlegung eines Produkts, einen enormen Rechenaufwand bedeuten kann.

Dies gilt insbesondere dann, wenn das Produkt wie beim RSA-Verfahren in seine Primfaktoren zerlegt werden muss. Gleiches gilt für die Exponentialfunktion, deren Berechnung vergleichsweise einfach erfolgt. Die Berechnung der inversen Exponentialfunktion wiederum weist eine sehr hohe Komplexität auf.

› Absicherung der asymmetrischen Substitution

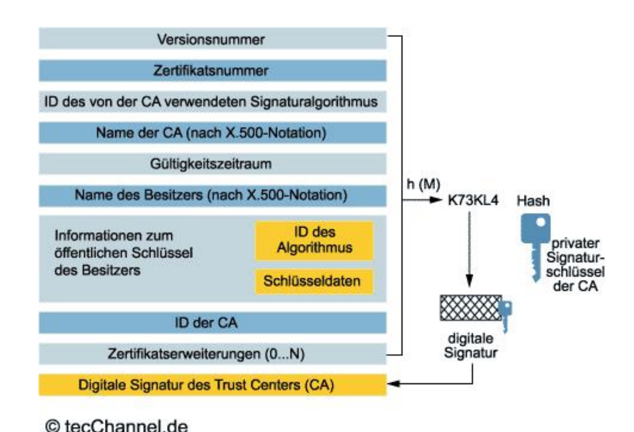
Eine deutliche Schwäche des Public-Key-Verfahrens besteht in der a priori nicht eindeutigen Zuordnung des öffentlichen Schlüssels zu seinem Besitzer. Auf diese Weise könnte sich ein "Man-in-the-Middle" so in die Kommunikation zwischen Alice und Bob einschalten, dass er Nachrichten von beiden entschlüsseln kann, ohne dass diese es bemerken.

Daher ist es von zentraler Bedeutung, dass die Information über den öffentlichen Schlüssel und den zugehörigen Besitzer von einer vertrauenswürdigen Quelle stammt. Hierzu existieren im Rahmen einer so genannten Public Key Infrastructure (PKI) verschiedene Möglichkeiten.

So kann man zum einen den öffentlichen Schlüssel über ein als sicher betrachtetes Medium übertragen. Darunter fällt speziell die persönliche Übergabe, aber auch die Übermittlung per Telefon, Brief oder Fax haben sich trotz aller Einschränkungen etabliert. Zum anderen besteht die Möglichkeit, sich die Identität des Schlüsselinhabers von einer Zertifizierungsstelle bestätigen zu lassen.

› Trust Center

Zur Überprüfung der Schlüsselinhaber dient meist eine Zertifizierungsinstanz (Englisch: Certification Authority (CA)), manchmal auch als Trust Center bezeichnet. Über die CA können sowohl Alice als auch Bob überprüfen, ob ein zur Beglaubigung eingereichter öffentlicher Schlüssel und eine Person mit einem eindeutigen Namen wirklich zusammengehören.



Aufbau eines Zertifikats: Die digitale Signatur der CA stellt sicher, dass der Schlüssel auch zum angegebenen Inhaber gehört.

Dazu verwalten Alice und Bob eine Liste von Zertifizierungsinstanzen, bei denen der Zusammenhang zwischen einem empfangenen öffentlichen Schlüssel und dessen Absender überprüft werden kann. Die Zertifizierungsinstanz stellt auf Anfrage ein Zertifikat nach dem ITU-Standard X.509 aus. Die obige Abbildung zeigt das in PKCS#6 definierte X.509-Format in der Version 3, das viele kryptographische Protokolle im Internet einsetzen.

Die Überprüfung des Schlüsselinhabers erfolgt in der Regel transparent für den Anwender. Nur wenn beim Trust Center kein öffentlicher Schlüssel hinterlegt wurde, müssen Alice oder Bob manuell entscheiden, ob sie die Kommunikation weiterführen

wollen.

Als weniger aufwendige Alternative zur Verwendung einer CA besteht die Möglichkeit, sich die Authentizität eines öffentlichen Schlüssels durch einen bereits bekannten, zertifizierten Kommunikationspartner bestätigen zu lassen. Diesen Weg nutzt beispielsweise PGP zum Aufbau eines so genannten Web of Trust.

› Hash-Funktionen

Die Bezeichnung Hash-Funktionen leitet sich vom englischen "to hash up" (zerhacken, zerkleinern, durcheinander bringen) ab. Synonym spricht man auch vom Message Digest (Engl. digest: Auslese, Auswahl) oder kurz MD. Eine Hash-Funktion generiert aus einer Zeichenfolge beliebiger Länge eine zweite Zeichenfolge fixer Länge. Diese zweite Zeichenfolge bezeichnet man als Message Authentication Code (MAC).

Eine Hash-Funktion muss dabei folgende Anforderungen erfüllen:

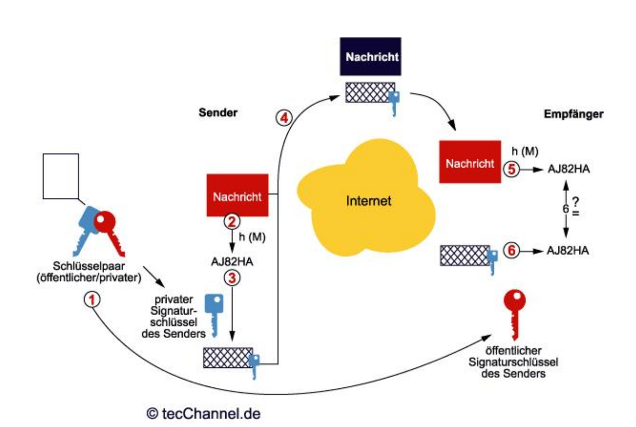
- Sie muss eindeutig sein. Eine identische Eingangszeichenfolge muss zur selben Zeichenfolge am Ausgang führen.
- Sie muss einfach zu berechnen sein.
- Ihre inverse Funktion muss schwierig zu berechnen sein. Ein Rückschluss aus der Ausgangszeichenfolge auf die Eingabe soll also möglichst aufwendig sein.
- Sie muss kollisionsresistent sein. Zwei unterschiedliche Eingangszeichenfolgen dürfen nach Möglichkeit nicht die gleiche Ausgabe hervorrufen.

Da Hashes nicht reversibel sind, lassen sie sich nicht zur Verschlüsselung einsetzen.

Dagegen leisten sie bei der Authentifizierung nützliche Dienste. So legt man Passwörter gern als MAC ab, damit sie auch der Administrator nicht als Klartext lesen kann. Das Login überprüft dann lediglich, ob der MAC des eingegebenen Passworts mit dem abgelegten Hash-Wert übereinstimmt. Auch für digitale Unterschriften (Digital Signatures) lässt sich ein MAC bestens einsetzen.

› Substitution vs. Signatur

Die Algorithmen asymmetrischer Verschlüsselung unterscheiden sich grundsätzlich, je nachdem, ob eine Nachricht verschlüsselt oder signiert werden soll.



Signieren mit dem Public Key: Der Absender unterzeichnet seine Nachricht mit dem Private Key. Mit dem Public Key kann der Empfänger die Authentizität der Unterschrift prüfen.

Bei der Substitution verschlüsselt der Sender die Nachricht mit dem öffentlichen Schlüssel des Empfängers, so dass dieser die Nachricht mit Hilfe seines privaten Schlüssels wieder in Klartext übersetzen kann.

Bei der Authentifizierung dagegen erzeugt der Absender mit Hilfe seines privaten Schlüssels eine Signatur, die der Empfänger unter Verwendung des öffentlichen Schlüssels des Senders verifizieren kann.

› Hybride Verschlüsselungsverfahren

Sowohl die symmetrischen als auch die asymmetrischen Kryptverfahren bringen ganz spezifische Vor- und Nachteile mit sich. Das legt den Gedanken nahe, in Anwendungslösungen zur Verschlüsselung beide Varianten zu verbinden.

Die daraus resultierenden hybriden Verschlüsselungen verbinden die Vorteile der symmetrischen und der asymmetrischen Methode: Also die hohe Effizienz auf der einen Seite und die Flexibilität und gesteigerte Sicherheit auf der anderen Seite.

Hierbei kommen in der Regel die symmetrischen Algorithmen zur Verschlüsselung größerer Datenmengen zum Einsatz. Der Austausch der hierzu notwendigen Schlüssel erfolgt dann über ein asymmetrisches Verfahren.

› Ende-zu-Ende vs. abschnittsweise Sicherheit

Ende-zu-Ende-Sicherheitsarchitekturen gehen davon aus, dass zwei Endgeräte einen sicheren Kanal aushandeln, aufbauen und aufrecht erhalten. Alternativ kann man aber nur kritische Übertragungsstrecken durch Verschlüsselung absichern. Ein Beispiel dafür wäre die Kommunikation zwischen zwei Mailservern, bei denen die lokale Datenübertragung mit den Mail-Clients unverschlüsselt erfolgt.

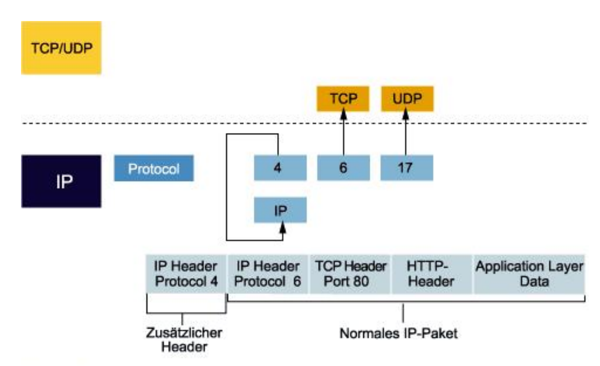
Die Vor- und Nachteile der beiden Architekturen sind offensichtlich:

- › Ende-zu-Ende-Sicherheit bietet in der Regel eine geringere Angriffsfläche, stellt aber meist hohe Anforderungen an die Rechenleistung und die Konfiguration der Endgeräte.
- › Abschnittsweise Sicherheit bietet mehr Gelegenheit für Attacken, beschränkt die

Notwendigkeit hoher Sicherheitsanforderungen aber auf die Gateways.

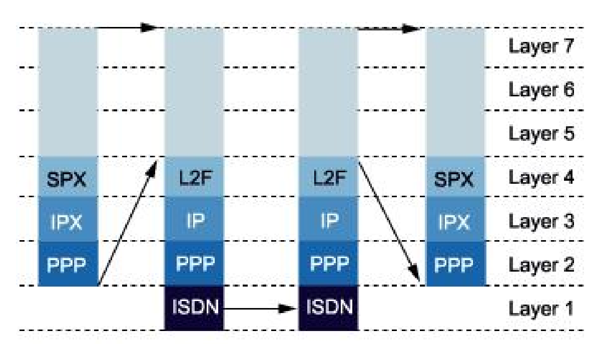
› Tunneling

Abschnittsweise Sicherheit wird heute meist über Tunneling realisiert. Darunter versteht man das mehrfache Einpacken eines Pakets auf einer Transportebene.



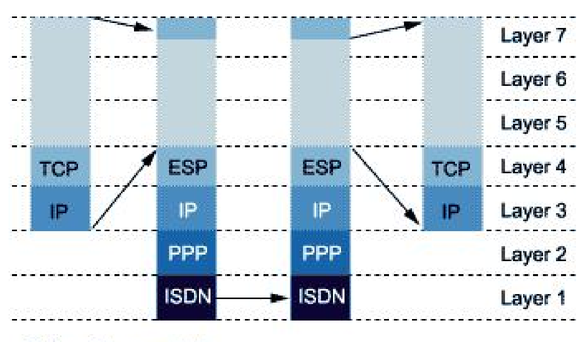
IP/IP-Tunneling: Für den Transport über klassische IP-basierte Netze kann man IPv6 über IPv4 tunneln.

Dazu ein kleines Beispiel: Ein TCP-Paket kann man in ein IP-Paket verpacken, indem man einen IP-Header mit den notwendigen Steuerinformationen (Quelladresse, Zieladresse, TTL et cetera) hinzufügt. Dabei setzt man das Type-Feld auf den Wert 6, damit das empfangende IP-Modul nach dem Entfernen des IP-Headers das TCP-Empfangsmodul aufruft.



Layer-2-Tunneling: Pakete der OSI-Schicht 2, meist PPP-Frames, werden in IP-Pakete verpackt. So tunnelt man üblicherweise alle Nicht-IP-Protokolle.

Beim Tunneln verpackt man nun das IP-Paket in ein weiteres, indem man einen zweiten IP-Header voranstellt. Damit beim Auspacken eine eindeutige Zuordnung erfolgen kann, setzt man das Type-Feld auf den Wert 4. Das empfangende IP-Modul ruft sich dann nach dem Entfernen des äußeren IP-Headers noch einmal auf.



Layer-3-Tunneling: Die Pakete der Vermittlungsschicht werden in IP-Frames verpackt. Bekanntestes Verfahren dieser Art ist IPsec.

So lässt sich das IP-Paket beispielsweise für normale Router anonymisieren, speziell auch mit anderen Ziel- und Quelladressen versehen.

› Angriffsverfahren

Sammelt ein Angreifer verschlüsselte Datenpakete, so kann er über verschiedene Techniken versuchen, Rückschlüsse auf den originalen Text zu ziehen. Meist steht ihm dazu nur die verschlüsselte Nachricht selbst zur Verfügung. Man spricht dann von einem Ciphertext-Angriff.

Dazu bieten sich verschiedene Möglichkeiten. Zum einen kann der Angreifer durch unmittelbares Ausprobieren aller Substitutionsmöglichkeiten versuchen, den Klartext zu rekonstruieren. Die Komplexität des Ausprobierens ist hierbei je nach verwendetem Kryptverfahren mehr oder weniger hoch. Um einen Einblick in die typische Komplexitätsbetrachtung kryptographischer Analyse zu geben, nehmen wir uns einmal die bereits zitierte Cäsar-Chiffre vor.

› Exhaustive Testing

Wenn wir im Rahmen einer monoalphabetischen Substitution ("Cäsar") jeden Buchstaben eines Alphabets mit 27 Buchstaben (26 plus ein Satzzeichen) einem beliebigen anderen zuordnen, erhalten wir:

- 27 Möglichkeiten für den ersten Buchstaben,
- 26 Möglichkeiten für den zweiten Buchstaben,
- 25 Möglichkeiten für den dritten Buchstaben,
- et cetera

Das entspricht 27 * 26 * .... * 2 * 1 = 27! oder rund 1,09*10e28 verschiedenen Zuordnungsmöglichkeiten. Nehmen wir einmal an, das Ausprobieren einer jeden Möglichkeit benötigte 1000 Maschinenzyklen auf einem Pentium-IV-Prozessor, der mit 2,5 GHz getaktet ist und bei jedem Oszillatortakt 4 Befehle ausführen kann. Dann dauerte das Durchprobieren aller Möglichkeiten ("Exhaustive Testing") rund 34,5 Billionen Jahre. Zum Vergleich: Der Urknall fand vor 13 bis 14 Milliarden Jahren statt, die Erde ist rund 4,5 Milliarden Jahre alt.

› Statistische Analyse

Allerdings lassen sich Verschlüsselungen nicht nur durch erschöpfendes Testen knacken. Ein schlauer Angreifer rückt Kryptverfahren durch gezieltes Ausnutzen der Schwachpunkte auf den Leib. So kann man beispielsweise den verschlüsselten Datenverkehr statistisch analysieren.

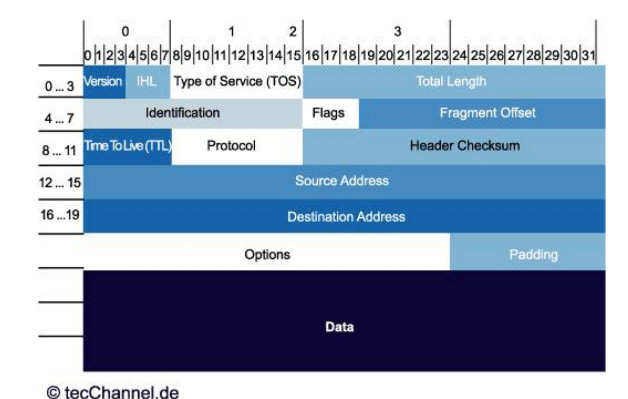
Im Fall unserer monoalphabetischen Verschlüsselung bedeutet das: Da hier jeder Buchstabe eines Alphabets einem bestimmten anderen zugeordnet wird, bleibt die Häufigkeit des Auftretens der einzelnen Buchstaben erhalten. Somit lassen sich durch eine einfache Häufigkeitsanalyse Rückschlüsse auf den ursprünglichen Text ziehen, sofern man dessen Sprache kennt oder erraten kann.

In deutschen Texten tritt etwa der Buchstabe "e" mit einer mittleren Wahrscheinlichkeit von 17,4 Prozent auf und übertrifft damit alle anderen Buchstaben weit. Findet man also in einem verschlüsselten Text einen Buchstaben, dessen Häufigkeit die der anderen deutlich übersteigt, handelt es sich sehr wahrscheinlich im Klartextalphabet um das "e". Auch Buchstabenpaare (Bigramme) treten mit unterschiedlichen Häufigkeiten auf: "en" ist beispielsweise mit 3,9 Prozent das häufigste Bigramm. Mit solchen Kenntnissen ausgestattet, kann ein Angreifer durch statistische Analyse monoalphabetische Codes sehr schnell entschlüsseln.

› Known oder Chosen Plaintext

Das Knacken von Schlüsseln und Kryptverfahren fällt einem Angreifer wesentlich leichter,

wenn er Teile des Klartexts bereits von vornherein kennt. So konnten die Alliierten im 2. Weltkrieg die Codes der deutschen Enigma (http://www.deutsches-museum.de/ausstell/meister/enigma.htm) -Chiffrierung unter anderem auf Grund stereotyper Meldungen brechen: Jeder chiffrierte Spruch begann beispielsweise mit der Buchstabengruppe ANX ("an:") und endete mit "HEILHITLER". Bei sehr kurzen Nachrichten durfte man getrost den Inhalt KEINEBESONDERENVORKOMMNISSE als sicher annehmen und konnte daraus den Tages-Code ermitteln.



Teilweise vorhersagbar: Speziell die Header-Daten von IP-Paketen lassen sich unschwer erraten oder ermitteln und ermöglichen so Known-Plaintext-Attacken.

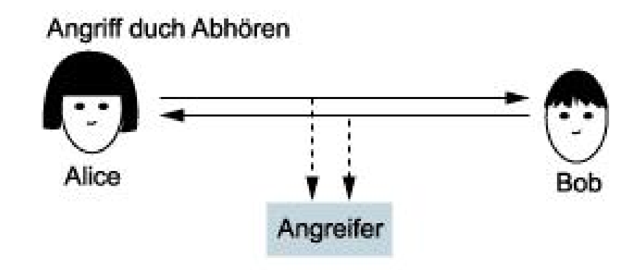
Diese Methode funktioniert auch für Datenpakete, bei denen speziell im Header Teile der Information vorhersagbar sind. In den IP-Kopfdaten findet sich an bekannten Stellen als Versionsangabe in der Regel "4" (IPv4), als Type of Service meist "0", als Protokollangabe oft "6" (TCP). Die auch im Header angegebene Paketlänge lässt sich schlicht nachzählen. Besteht zusätzlich die Möglichkeit, den Verkehr nach verschiedenen Routern abzuhören, kennt man auch den Inhalt des TTL-Felds (Anzahl der Hops).

In anderen Fällen besteht für den Angreifer sogar die Möglichkeit, selbst gewählten Text nach den gleichen Regeln wie ein berechtigter Nutzer verschlüsseln zu lassen. Kann der Angreifer anschließend den verschlüsselten Text abhören, besteht natürlich die Möglichkeit, Rückschlüsse über den Verschlüsselungsalgorithmus zu ziehen. Auch dafür ein Beispiel aus dem letzten Krieg: In einem bekannten Fall bombardierte die britische Luftwaffe eine Markierungsboje, um die vorhersagbare Enigma-chiffrierte Meldung ERLOSCHENISTLEUCHTTONNE zu provozieren. Tages-Code geknackt ...

› Angriffsarten

Ein Angreifer kann verschiedenste Möglichkeiten nutzen, um an die Information einer verschlüsselten Nachricht zu kommen, die von einem Sender A (gern als "Alice" apostrophiert) an einen Empfänger B ("Bob") geschickt wird.

Die gängigste Methode ist die des Abhörens. Nach dem englischen Verb to eavesdrop (heimlich lauschen, horchen) nennt man Lauscher "Eve". In Netzen, die über Hubs verbunden sind, hört der Angreifer am leichtesten mit: Jedes Datenpaket wird ja an jedem Port ausgegeben. Aber auch in per Switches oder Router gekoppelten Netzen können - etwa über Manipulation der Adresstabellen - Datenpakete abgefangen oder umgeleitet werden.



Die gängigsten Attacken: Der Angreifer hört die übermittelten Nachrichten passiv mit oder schaltet sich aktiv zwischen Absender und Empfänger.



Über die gezielte Manipulation des Datenverkehrs erfolgt auch der Man-in-the-Middle-Attack. Der Angreifer - hier nennt man ihn "Mallory" - schaltet sich zwischen Alice und Bob. So kann er Alices Pakete abfangen und mitlesen, bei Bedarf modifizieren und dann an Bob weiter senden. Verhält Mallory sich dabei konsistent, meinen Alice und Bob, dass sie unmittelbar miteinander kommunizieren. Mallory hat nun die Gelegenheit, die Wahl der Kryptverfahren oder die Auswahl der Keys so zu beeinflussen, dass er die Nachrichten von Alice und Bob mitlesen kann.

Replay-Attacken basieren darauf, kritische Teile einer Kommunikation aufzuzeichnen und sie später wieder abzuspielen. So kann es etwa dem Angreifer gelingen, eine Login-Prozedur zu simulieren und auf diese Weise Passwörter herauszufinden.

Während die vorangegangenen Verfahren eine gewisse Eleganz aufweisen, können Angriffe auch mit nackter Gewalt ("brute force") erfolgen. Der Angreifer bombardiert den Zielrechner beispielsweise mit einer so großen Anzahl von Anfragen, dass keine Ressourcen mehr für die Erfüllung der eigentlichen Aufgabe zur Verfügung stehen.

› Ausblick

Im vorliegenden ersten Teil unserer Artikelserie zum Thema Security haben wir einige Basisdefinitionen abgeklärt und uns näher mit den Grundlagen der Kryptologie und Kryptanalyse vertraut gemacht.

Applications	s-MIME Kerberos Proxies SET IPsec (ISAKMP)
TCP/UDP (Transport)	SOCKS SSL,TLS
IP (Internetwork)	IPsec (AH, ESP) Packet filtering Tunneling protocols
Network Interface (Data Link)	CHAP, PAP, MS-CHAP

© tecChannel.de

Das Programm: In den nächsten Folgen kommen die gängigsten Security-Verfahren auf den verschiedenen Netzwerkschichten zur Sprache.

Davon ausgehend nehmen wir im nächsten Teil (http://www.tecchannel.de/software/1095/index.html) der Serie die gängigsten Verfahren zur rechnergestützten Verschlüsselung näher unter die Lupe. Insbesondere wollen wir uns ansehen, für welche Einsatzgebiete RC4, MD5, DES, IDEA, RSA, Diffie-Hellman, SHA und DHA in Frage kommen, wie sicher sie sind, und welche Performance-Trade-offs man für die entsprechende Security in Kauf nehmen muss. (jlu (http://www.tecchannel.de/impressum/jluther.html))

Grundlagen: Security

Teil 1	Einführung in die Kryptographie
Teil 2	Kryptologische Verfahren
Teil 3	Security auf dem Link Layer
Teil 4	Security auf dem Network Layer
Teil 5	Security auf dem Application Layer
Teil 6	Security mit VPNs

› Weitere Themen zu diesem Artikel:

- Security im Überblick (Teil 2) (http://www.tecchannel.de/software/1095/index.html)
- Security im Überblick (Teil 3) (http://www.tecchannel.de/software/1144/index.html)
- Security im Überblick (Teil 4) (http://www.tecchannel.de/software/1168/index.html)
- Security im Überblick (Teil 5) (http://www.tecchannel.de/software/1194/index.html)
- Kryptographie-Grundlagen (http://www.tecchannel.de/internet/416/index.html)
- Praxis der digitalen Signatur (http://www.tecchannel.de/internet/909/index.html)
- Sicherheit im WLAN (http://www.tecchannel.de/hardware/928/index.html)
- Firewall-Grundlagen (http://www.tecchannel.de/internet/682/index.html)
- Ausfallsichere Systeme (http://www.tecchannel.de/hardware/422/index.html)
- Sichere E-Mail (http://www.tecchannel.de/internet/398/index.html)
- Lauschangriff im Firmennetz (http://www.tecchannel.de/internet/288/index.html)

Security im Überblick (Teil 2)

› Die Rechner- und Netzsicherheit wird immer mehr zum zentralen IT-Faktor im Unternehmen. Im zweiten Teil unserer Security-Serie beschäftigen wir uns mit den wichtigsten kryptographischen Verfahren.

› VON AXEL SIKORA

Das Wort Kryptographie ist aus den griechischen Wörtern krypto (versteckt, geheim) und graph (Schrift, Wort) entlehnt. Damit bedeutet Kryptographie im Ursprung so viel wie Geheimschrift. Sie behandelt zum einen die Verschlüsselung (encryption), also die Transformation einer verständlichen Informationsdarstellung (Klartext, plain text) in eine nicht verständliche Darstellung (Geheimtext, cipher text). Diese muss so erfolgen, dass die angewandte Transformation im Rahmen einer Entschlüsselung (decryption) von Befugten wieder eindeutig rückgängig gemacht werden kann.

Im erweiterten Sinne zählen zur Kryptographie auch Aufgaben der Integritätsprüfung und Authentifizierung. Oft basieren entsprechende Funktionen auf eingeschränkten kryptographischen Verfahren (Hash-Funktionen), bei denen die Verschlüsselung nicht unbedingt rückgängig gemacht werden muss. Es gilt lediglich sicherzustellen, dass zwei unterschiedliche Eingaben nur mit einer sehr geringen Wahrscheinlichkeit das gleiche Ergebnis liefern.

Grundlagen: Security

Teil 1	Einführung in die Kryptographie
Teil 2	Kryptologische Verfahren
Teil 3	Security auf dem Link Layer
Teil 4	Security auf dem Network Layer
Teil 5	Security auf dem Application Layer
Teil 6	Security mit VPNs

› Symmetrische Verschlüsselungsverfahren

Exemplarisch für symmetrische Verschlüsselungsverfahren sehen wir uns drei Beispiele an: Die Verknüpfung mit Hilfe einer logischen Exklusiv-Oder-Funktion, den darauf aufbauenden RC-4-Algorithmus sowie den Data Encryption Standard (DES).

Der einfachste Einsatz symmetrischer Schlüssel basiert auf der logischen Exklusiv-Oder-Funktion. Die zweifache XOR-Verknüpfung eines Zeichens A mit einem Zeichen B hat wieder das ursprüngliche Zeichen A zum Ergebnis. Das zweifache Exklusiv-Oder mit einem identischen Zeichen entspricht also der inversen Verknüpfung:

$$\begin{aligned} (A \oplus B) \oplus B &= A \oplus (B \oplus B) && \text{Assoziativgesetz} \\ &= A \oplus 0 && \text{Eigenschaft von XOR} \\ &= A && \text{Eigenschaft von XOR} \end{aligned}$$

Zur verschlüsselten Übertragung verknüpft der Sender ein Zeichen A mit einem Schlüssel B per XOR und übersendet dann das Resultat. Der Empfänger verknüpft das empfangene Zeichen erneut mit dem Schlüssel B und erhält dann das ursprüngliche Zeichen A.

› RC-4

RC-4 wurde 1987 von dem bekannten Kryptographen Ron Rivest entwickelt. Das Kürzel RC steht für Rivest Cipher. Es handelt sich um ein einfaches und schnelles Stromverschlüsselungsverfahren, das auf der schon beschriebenen XOR-Verknüpfung basiert. Da sich der Algorithmus sehr gut zur Implementation in Software eignet, kam RC-4 schon bald in zahlreichen kommerziellen Produkten zum Einsatz, darunter Lotus Notes, Oracle Secure SQL und Netscape Navigator.

Die Stärke des Algorithmus besteht darin, dass mit einem sehr einfachen Verfahren aus dem eingegebenen Schlüssel S ein langer, pseudo-zufälliger interner Schlüssel P erzeugt wird. Diesen nutzt RC-4 dann zur Chiffrierung des Klartexts. Besteht der Schlüssel S aus n Bytes von S(0) bis S(n-1), dann initialisiert man:

» *i, j = 0*
» *P[k] = k mit k=0,...,256*

und berechnet 256 Mal:

» *j = j+P[i]+S[i] mod 256*
» *vertausche P[i] und P[j]*
» *i = i+1 mod n*

Das zur Ver- respektive Entschlüsselung des Nachrichten-Bytes i notwendige Schlüssel-Byte K[i] berechnet sich nach der Vorschrift:

» *i = i+1 mod 256*
» *j = j+P[i] mod 256*
» *vertausche P[i] und P[j]*
» *t = P[i]+P[j] mod 256*
» *K[i] = P[t]*

Über die Variablen i und j sowie die Permutation P speichert RC-4 also 258 verschiedene Zustandsinformationen. 256 der Bytes sind Permutationen von 0, ...,255 und somit gleich verteilt.

› DES

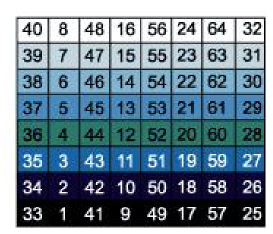
Der Data Encryption Standard (DES) wurde Mitte der 70er Jahre von IBM entwickelt, 1977 vom US-amerikanischen National Bureau of Standards vorgestellt und 1979 vom National Institute of Standards and Technology (NIST (http://www.nist.gov/)) als Standard verabschiedet.

DES gehört zur Familie der Blockchiffren und teilt eine Nachricht in 64 Bit große Datenblöcke auf. Auf der Verschlüsselungsseite umfasst es drei Bearbeitungsschritte, die wieder den originalen Text liefern, wenn sie auf der Entschlüsselungsseite identisch durchgeführt werden.

DES zählt zu den heute immer noch am weitesten verbreiteten Verschlüsselungsalgorithmen. Zwar gilt der Ur-Algorithmus inzwischen nicht mehr als zeitgemäß. Die aktuelle Variante Triple-DES (3DES) jedoch führt die Verschlüsselung drei Mal hintereinander aus, was zu einer exponentiellen Steigerung der Sicherheit führt. 3DES findet vielfach Anwendung im Bereich der Finanzdienstleistungen.

› Permutationen

DES besteht sowohl bei der Verschlüsselung als auch bei der Entschlüsselung aus den drei Bearbeitungsschritten initiale Permutation, Ver-/Entschlüsselung in mehreren Runden sowie finale Permutation.



Initiale Permutation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Finale Permutation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

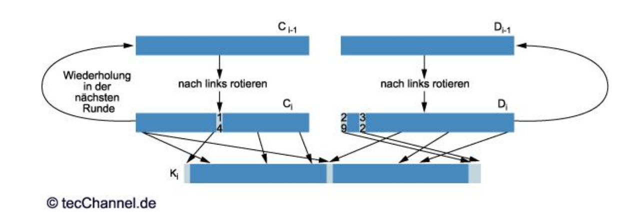
Bäumchen wechsle dich: In den Permutationsschritten kippt DES jeweils die Zeilen-/Spalten-Matrix der Bits.

Die Permutationen vor der ersten und nach der letzten Runde dienen keinerlei erkennbarem kryptologischen Zweck. Da DES ursprünglich zur Implementation in Hardware entwickelt wurde, vermutet man, dass die Umstellung der Bits zur Anpassung an die schmalen Register der 70er-Jahre-CPUs diente.

Bei der finalen Permutation handelt es sich schlicht um eine Inverse der initialen Permutation. Nach Durchführung der initialen und der finalen Permutation steht ein Bit also einfach wieder an der ursprünglichen Stelle.

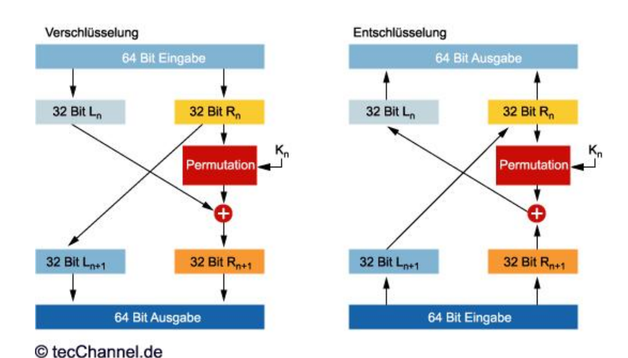
› Verschlüsselung

Die DES-Verschlüsselung basiert auf einem 64 Bit langen Schlüssel. Davon sind aber nur 56 Bit kryptographisch relevant, da es sich bei jedem achten Bit um ein Parity-Bit handelt. DES erzeugt aus diesen 64 Bit 16 verschiedene, je 48 Bit lange Schlüssel.



DES-Schlüsseltransformation: Sie sorgt für die Verwendung unterschiedlicher Schlüsselbits in jeder Runde.

Dazu bildet es aus den 56 relevanten Bits mit Hilfe einer Permutation zwei 28 Bit lange Muster C[i-1] und D[i-1]. Anschließend rotiert DES diese beiden Teilschlüssel rundenabhängig um ein oder zwei Bit nach links. In den Phasen 1, 2, 9 und 16 wird um ein Bit geshiftet, in den anderen Runden um zwei Bit. Die so erzeugten Schlüssel C[i] und D[i] werden zu den neuen Schlüsseln C[i-1] und D[i-1]. Schließlich stellt eine weitere Permutation aus C[i] und D[i] zwei 24 Bit lange Folgen zusammen, die in Kombination zum Schlüssel K[n] werden.



Blockbasiert: DES verschlüsselt den Klartext in 64-Bit-Häppchen.

Für die Verschlüsselung teilt DES den Klartext nun in jeweils 64 Bit lange Blöcke auf. Diese splittet es nochmals in zwei 32 Bit lange Bestandteile L[n] und R[n]. R[n] wird über eine so genannte Mangler-Funktion vermischt. Dazu kommt eine tabellenbasierte Umrechnung auf der Grundlage der Eingangsvariablen R[n] und des Schlüssels K[n] zum Einsatz.

› IDEA

Der International Data Encryption Algorithm (IDEA) wurde Anfang der Neunziger Jahre von Xuejia Lai und James Massey an der ETH Zürich (http://www.ethz.ch/) entwickelt und 1991 veröffentlicht. Er zählt ebenfalls zu den Blockchiffren, wendet allerdings einen 128 Bit großen Schlüssel auf die 64 Bit großen Datenpakete des Klartextes an.

IDEA beruht auf der Mischung dreier mathematischer Funktionen, die jeweils auf 16-Bit-Blöcke des Texts angewendet werden. Neben der schon bekannten XOR-Funktion kommt eine Addition modulo 2^16 zum Einsatz, die zwei Blöcke unter Verwerfen des Übertrags addiert. Bei der dritten Funktion handelt es sich um eine Multiplikation modulo 2^16+1, die zunächst zwei Blöcke multipliziert und das Resultat dann durch 2^16+1 dividiert. Der Rest wird als 16-Bit-Ergebnis übernommen.

IDEA verknüpft diese drei Operationen zu einem recht komplizierten Netzwerk, das in insgesamt acht Runden durchlaufen wird. Trotz der komplizierteren Verfahrensweise operiert IDEA (als Software-Implementation) schneller als DES und gilt gleichzeitig als sicherer gegen Kryptangriffe.

› Asymmetrische Verschlüsselungsverfahren

Während symmetrische Verfahren mit einem identischen Key zur Ver- und Entschlüsselung arbeiten, setzen die auch als Public-Key-Verfahren bezeichneten asymmetrischen Methoden auf zwei unterschiedliche Schlüssel.

Der eine Schlüssel heißt privater Schlüssel (private key), der zugehörige Algorithmus Dechiffrier-Algorithmus. Den anderen Schlüssel nennt man öffentlichen Schlüssel (public key), den entsprechenden Algorithmus Chiffrier-Algorithmus. Dabei lässt sich aus dem public key nicht auf den private key schließen. Daher kann man den public Key ohne Gefahr öffentlich bekannt machen. Er ist von Dritten zur Verschlüsselung von Nachrichten nutzbar, die anschließend nur der Besitzer des zugehörigen private key wieder dechiffrieren kann.

Bekanntester Vertreter der Public-key-Verfahren ist der nach den Initialen seiner Entwickler Ron Rivest, Adi Shamir und Leonard Adleman benannte RSA-Algorithmus. Er basiert auf der Grundlage, dass die Multiplikation zweier Zahlen eine einfache Operation darstellt, während der umgekehrte Vorgang, also die Faktorzerlegung eines Produkts, einen enormen Rechenaufwand bedeutet. Dies gilt insbesondere dann, wenn das Produkt in seine Primfaktoren zerlegt werden muss.

› RSA

Der RSA-Algorithmus basiert auf folgenden vier Schritten:

- › Wähle zwei große Primzahlen p und q, die geheim bleiben.
- › Berechne das Produkt n = p*q. n wird als Modulus bezeichnet.
- › Um einen öffentlichen Schlüssel zu erzeugen, wähle eine Zahl e kleiner n, die teilerfremd zur Eulerschen Funktion E(n) = (p-1)*(q-1) ist. Das bedeutet, dass e und E(n) keinen gemeinsamen Teiler außer 1 besitzen. [e,n] ist der öffentliche Schlüssel.
- › Um den privaten Schlüssel zu erzeugen, bestimme eine Zahl d = e^-1 mod E(n). Dann gilt: e*d = 1 mod E(n). [d,n] ist der private Schlüssel.

Bei der Verschlüsselung kommt der RSA-Algorithmus folgendermaßen zum Einsatz:

- › Alice verschlüsselt ihren Klartext m gemäß c = m^e mod n und sendet ihn an Bob. In diesem Fall ist [e,n] der öffentliche Schlüssel von Bob.
- › Bob entschlüsselt den Geheimtext c mit seinem privaten Schlüssel [d,n] gemäß m = c^d mod n und erhält auf Grund des Zusammenhangs von d und e den Klartext m.

Wie man sieht, führt der Empfänger bei der Entschlüsselung die gleiche Operation durch wie der Sender bei der Verschlüsselung. In ähnlicher Weise lässt sich der RSA-Algorithmus zur Erzeugung und Überprüfung von Signaturen einsetzen:

- › Alice sendet eine signierte Nachricht, indem sie s = m^d mod n erzeugt und überträgt. [d,n] ist in diesem Fall der private Schlüssel von Alice.
- › Bob entschlüsselt die Signatur gemäß m = s^e mod n und erhält auf Grund des Zusammenhangs von d und e den Klartext m. [e,n] ist in diesem Fall der öffentliche Schlüssel von Alice. So kann jeder überprüfen, dass nur Alice die Signatur erzeugt hat.

› Diffie-Hellman

Der nach seinen Erfindern benannte Diffie-Hellman-Algorithmus (DH) dient der Vereinbarung eines gemeinsamen symmetrischen Schlüssels über einen unsicheren Kanal. Wie RSA basiert auch DH auf einem öffentlichen und einem privaten Schlüssel:

- › Beiden an der sicheren Kommunikation beteiligten Partnern Alice und Bob sind eine große Primzahl p und ein ganzzahliger Wert g (Generator) frei zugänglich.
- › Alice generiert eine große Zufallszahl a, berechnet eine Zahl A = g^a mod p.
- › Bob generiert ebenfalls eine große Zufallszahl b, berechnet eine Zahl B = g^b mod p und sendet B an Alice.
- › Alice berechnet eine Zahl K[1] = B^a mod p.
- › Bob berechnet eine Zahl K[2] = A^b mod p.

Beide Zahlen K[1] und K[2] sind gleich, es gilt: K = K[1] = K[2] = g^a*b mod p. K wird nun als geheimer symmetrischer Schlüssel verwendet, der ohne Kenntnis von a und b nicht berechnet werden kann.

› Man in the Middle

Der grundlegende Diffie-Hellman-Algorithmus gibt lediglich Sicherheit gegen passives Abhören. Ein Man-in-the-Middle-Angriff kann hingegen sowohl Alice als auch Bob suggerieren, dass nur sie miteinander sprächen. Ein solcher Angriff könnte folgendermaßen verlaufen:

- › Die beiden Zahlen p und g sind nicht nur Alice und Bob, sondern auch dem Angreifer Mallory frei zugänglich.

- Alice versendet die Zahl A=g^a mod p. Mallory empfängt A, sendet aber M = g^m mod p an Bob weiter.
- Bob versendet die Zahl B = g^b mod p. Mallory empfängt B, sendet aber M = g^m mod p an Alice weiter.
- Alice berechnet nun ihre Zahl K[1] = M^a mod p. Mallory kann diesen Schlüssel ebenfalls durch K[1m] = K[1] = A^m mod p berechnen.
- Bob berechnet eine Zahl K[2] = M^b mod p. Mallory kann auch diesen Schlüssel durch K[2m] = K[2] = B^m mod p berechnen.

Mallory kann nun alle Nachrichten von Alice an Bob aufnehmen, mit K[1m] entschlüsseln, mit K[2m] erneut verschlüsseln und dann an Bob weiterleiten. Gleiches tut er umgekehrt mit den Nachrichten von Bob an Alice. Sowohl Alice als auch Bob glauben, unmittelbar miteinander zu kommunizieren.

Das funktioniert aber nur, wenn Mallory die Möglichkeit hat, bei der Verteilung des öffentlichen Schlüssels eine Manipulation vorzunehmen. Wird der öffentliche Schlüssel authentifiziert oder über ein zuverlässiges Medium übertragen, dann ist der Diffie-Hellman-Algorithmus gegen solche Angriffe geschützt.

› Einweg-Hash-Funktionen

Hash-Funktionen sind in der Informatik seit langem bekannt. Sie dienen beispielsweise bei Datenbank-Anwendungen zur einfachen Indizierung und somit dem schnellen Wiederauffinden von Informationen. Dazu fassen sie umfangreiche Informationen - wie etwa Kundennamen - durch Bilden irgendeiner Art von Quersumme zu einer komprimierten, leichter verwaltbaren Information zusammen. Letztere nennt man den Hash-Wert der Information. Die verwendete Hash-Funktion muss natürlich sicherstellen, dass für verschiedene Eingangsinformationen auch hinreichend unterschiedliche Hash-Werte entstehen.

Solche Hashes lassen sich auch gut zur Authentifizierung und Signatur einsetzen, falls der verwendete Algorithmus zwei zusätzliche Kriterien erfüllen kann. Zum einen darf es nicht möglich sein, mit vertretbarem Aufwand aus dem Hash-Wert die Originalinformation zu rekonstruieren. Zum Zweiten muss es aus Gründen der Fälschungssicherheit ausgeschlossen sein, mit vertretbarem Aufwand aus einer gegebenen Originalinformation eine zweite Information zu generieren, die denselben Hash-Wert ergäbe ("Kollision").

Einweg-Hash-Funktionen werden unter anderem auch als Kompressionsfunktion, Message Digest, kryptographische Prüfsumme oder Message Integrity Check (MIC) bezeichnet. Schon daraus lässt sich das breite Einsatzspektrum ersehen. Da Einweg-Hash-Funktionen für jedermann berechenbar sein sollen, verwenden sie keine geheimen Schlüssel. Den Hash-Wert einer Einweg-Funktion bezeichnet man als Message Authentication Code (MAC).

› MD-5

Zu den am weitesten verbreiteten Message-Digest-Funktionen zählt MD-5. Es gehört mit MD-2 und MD-4 zu einer Familie stetig verbesserter Hash-Funktionen, die von dem bereits mehrfach zitierten Ron Rivest entwickelt wurde.

MD-5 verarbeitet Nachrichten in 512-Bit-Blöcken, indem es jeweils sechzehn 32-Bit-Blöcke zusammenfasst. Auf Grund dieser Eigenschaft eignet sich MD-5 besonders für den Einsatz auf 32-Bit-Prozessoren. Auch als MAC erhält man einen 128 Bit langen Block aus vier 32-Bit-Blöcken.

Die Verarbeitung findet bei MD-5 in mehreren Stufen statt, wobei als Eingangsfolge jeder Stufe ein 512 Bit langer Block der Nachricht und das MAC der vorangegangenen Stufe dienen. Für die erste Stufe wird ein initialer MAC mit den vier 32-Bit-Blöcken d0 = 6745230116, d1 = efcdab8916, d2 = 98badcfe16 und d3 = 1032547616 verwendet. Beim MAC der letzten Stufe handelt es sich dann um den gültigen Message Digest.

› SHA-1

Zu den Schwächen des MD-5-Algorithmus zählt, dass sich entgegen der Anforderung an Einweg-Hash-Funktionen relativ schnell Kollisionen der Hash-Werte ergeben können. Diesem Umstand versucht der 1994 von NIST (http://www.nist.gov/) vorgeschlagene Secure Hash Algorithm SHA-1 abzuhelfen.

SHA-1 generiert aus einer maximal 2^64 Bit langen Eingangsfolge eine 160 Bit lange Zeichenfolge. Dabei arbeitet es mit 512-Bit-Blöcken. Der Algorithmus verwendet fünf Stufen, wobei auf jeder Stufe 80 Schritte ausgeführt werden. Wie MD-5 nutzt auch SHA-1 anfangs einen vorgegebenen, initialen Message Digest.

Auf Grund seiner längeren Ergebnisfolge besteht bei SHA-1 eine wesentlich geringere Wahrscheinlichkeit für eine Kollision als bei MD-5. Während bei MD-5 durchschnittlich nach 2^64 Operationen eine Kollision entsteht, ist dies bei SHA-1 erst alle 2^80 Operationen der Fall.

› DSA

Aus dem mit Hilfe einer Hash-Funktion generierten Message Authentication Code lässt sich eine digitale Unterschrift erzeugen, indem man ihn mit einem privaten Schlüssel chiffriert. Auf diesem Weg arbeitet etwa der Digital Signature Algorithm (DSA) des Digital Signature Standard (DSS (http://www.itl.nist.gov/fipspubs/fip186.htm)). Er zeigt ein mögliches Vorgehen auf der Grundlage eines mit SHA-1 erzeugten MAC:

- Es wird eine große Primzahl p ausgewählt, die typisch zwischen 512 und 1024 Bits lang ist.
- Es wird ein Primfaktor q der Zahl (p-1) berechnet. q ist 160 Bits lang.
- Es wird eine Zahl g berechnet mit g = h^(p-1/q) mod p, wobei h kleiner p und g größer 1.
- Es wird eine weitere Zahl x als privater Schlüssel des Senders Alice ausgewählt, wobei x kleiner q.
- Die Zahl y = g^x mod p wird nun als öffentlicher Schlüssel verwendet.
- Alice unterzeichnet ihre Mitteilungen nun mit r = (g^k mod p) mod q sowie s = (k^-1*(SHA1(m)+x*r)) mod q.

Alice versendet nun (m, r, s). Der Empfänger Bob überprüft die digitale Unterschrift mit Hilfe von:

- w = s^-1 mod q
- u(1) = (SHA1(m)*w) mod q
- u(2) = (r*w) mod q
- v = ((g^u(1)*g^u(2)) mod p) mod q

Falls v = r ist, gilt die Unterschrift von Alice als bestätigt.

› Ausblick

In den ersten beiden Teilen unserer Artikelserie zu Security haben wir einige Basisdefinitionen abgeklärt und uns näher mit den verschiedenen Verschlüsselungs- und Authentifizierungsverfahren vertraut gemacht.

Applications	s-MIME Kerberos Proxies SET IPsec (ISAKMP)
TCP/UDP (Transport)	SOCKS SSL,TLS
IP (Internetwork)	IPsec (AH, ESP) Packet filtering Tunneling protocols
Network Interface (Data Link)	CHAP, PAP, MS-CHAP

© tecChannel.de

Das Programm: In den nächsten Folgen kommen die gängigsten Security-Verfahren auf den verschiedenen Netzwerkschichten zur Sprache.

Davon ausgehend nehmen wir im nächsten Teil der Serie die wichtigsten Sicherheitsprotokolle auf dem Link Layer des Netzwerks näher unter die Lupe. Dazu zählen unter anderem PPP, PAP und CHAP, die Tunneling-Protokolle PPTP sowie L2TP und nicht zuletzt moderne RAS-Security-Verfahren wie RADIUS/TACACS und IEEE 802.1x. (jlu (http://www.tecchannel.de/impressum/jluther.html))

Grundlagen: Security

Teil 1	Einführung in die Kryptographie
Teil 2	Kryptologische Verfahren
Teil 3	Security auf dem Link Layer
Teil 4	Security auf dem Network Layer
Teil 5	Security auf dem Application Layer
Teil 6	Security mit VPNs

› Weitere Themen zu diesem Artikel:

- Security im Überblick (Teil 1) (http://www.tecchannel.de/software/1068/index.html)
- Security im Überblick (Teil 3) (http://www.tecchannel.de/software/1144/index.html)
- Security im Überblick (Teil 4) (http://www.tecchannel.de/software/1168/index.html)
- Security im Überblick (Teil 5) (http://www.tecchannel.de/software/1194/index.html)
- Kryptographie-Grundlagen (http://www.tecchannel.de/internet/416/index.html)
- Praxis der digitalen Signatur (http://www.tecchannel.de/internet/909/index.html)
- Sicherheit im WLAN (http://www.tecchannel.de/hardware/928/index.html)
- Sichere E-Mail (http://www.tecchannel.de/internet/398/index.html)
- Lauschangriff im Firmennetz (http://www.tecchannel.de/internet/288/index.html)

Security im Überblick (Teil 3)

› Auf dem Data Link Layer tummeln sich eine ganze Reihe bekannter Authentifizierungs- und Sicherheitsprotokolle von PAP und CHAP über L2TP bis hin zu RADIUS, TACACS und IEEE 802.1x.

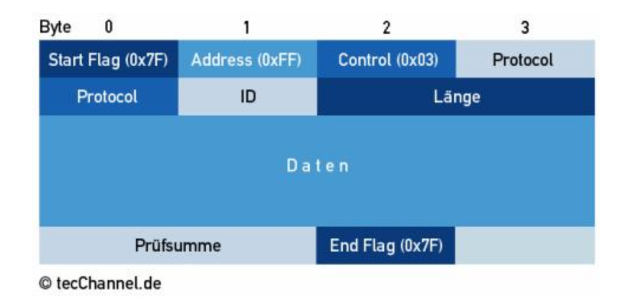
› VON AXEL SIKORA

Auf der Ebene 2 des OSI-Referenzmodells, dem Data Link Layer, lassen sich verschiedene Maßnahmen zur Erhöhung der Sicherheit einsetzen. Dazu zählen zum einen Authentifizierungsprotokolle, wie sie beim Aufbau von PPP-Verbindungen eingesetzt werden. Daneben existieren unterschiedliche Tunnelprotokolle, die in der Regel die Punkt-zu-Punkt-Verbindungen des Point-to-Point Protocol (PPP) tunneln. Sie werden ergänzt von Port-basierten Protokollen, die auf der Grundlage der Authentifizierung die Nutzung eines Ports freischalten. Als grundlegendes Protokoll dient in der Regel PPP, das meist für Wählverbindungen ins Internet (Dial-up Access) zum Einsatz kommt.

Grundlagen: Security

› Authentifizierung in PPP

Beim Point-to-Point Protocol (PPP) handelt es sich um ein so genanntes "Multiprotokoll-Protokoll", das sich aus vielen Teilprotokollen zusammensetzt. Es wurde ursprünglich in RFC 1548 (http://www.ietf.org/rfc/rfc1548.txt) (PPP) und RFC 1172 (http://www.ietf.org/rfc/rfc1172.txt) (The PPP Initial Configuration Options) beschrieben.



TCP/IP über serielle Verbindungen: Das Rahmenformat des Point-to-Point Protocol PPP.

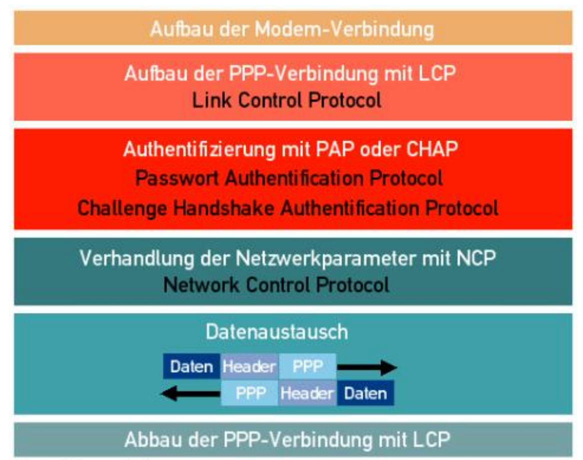
Beide wurden 1994 durch RFC 1661 (http://www.ietf.org/rfc/rfc1661.txt) (PPP), RFC 1662 (http://www.ietf.org/rfc/rfc1662.txt) (PPP in HDLC-like Framing) und RFC 1663 (http://www.ietf.org/rfc/rfc1663.txt) (PPP Reliable Transmission) ersetzt. Später wurde mit RFC 1962 das PPP Compression Control Protocol (CCP) hinzugefügt. Das Rahmenformat von PPP zeigt oben stehende Abbildung.

Besondere Bedeutung im Zusammenhang mit der hier geführten Sicherheitsdiskussion haben das PPP Authentication Protocol (PAP, RFC 1334 (http://www.ietf.org/rfc/rfc1334.txt))

und das PPP Challenge Handshake Authentication Protocol (CHAP, RFC 1994 (http://www.ietf.org/rfc/rfc1994.txt)), das in einer verwandten Realisierung auch von Microsoft als Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP v2, RFC 2759 (http://www.ietf.org/rfc/rfc2759.txt)) vorliegt.

› Ablauf

Den Ablauf des Verbindungsaufbaus mit PPP zeigt die unten stehende Abbildung. Bei der Authentifizierung unter PPP handelt es sich grundsätzlich um einen einseitigen Vorgang, da sich nur der Anrufer ausweisen muss. Der angerufene Knoten überprüft die Authentifizierung. Er selbst authentifiziert sich lediglich durch seine Verfügbarkeit unter der physischen Verbindung, also zum Beispiel durch die entsprechende Telefonnummer.



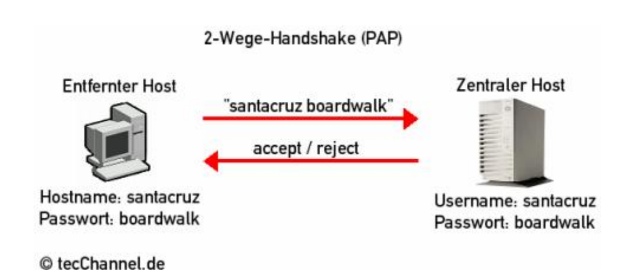
Aufbau, Authentifizierung, Datenaustausch: Der Ablauf einer typischen PPP-Verbindung.

Diese manchmal auch als physische Authentifizierung bezeichnete Vorgehensweise eignet sich jedoch offensichtlich nur für zuverlässige Netze. Sie birgt Gefahren, wenn die eindeutige Erreichbarkeit nicht sichergestellt werden kann. In einem öffentlichen IP-Netzwerk lässt sich beispielsweise nicht ausschließen, dass IP-Adressen oder Routen manipuliert wurden.

Die Stellung von PPP im OSI-Referenzmodell ist zwiespältig. Zum einen eignet sich PPP für die Übertragung verschiedener Netzwerkprotokolle. So beschreiben RFC 1331 (http://www.ietf.org/rfc/rfc1331.txt) und RFC 1332 (http://www.ietf.org/rfc/rfc1332.txt) die Übertragung von IP mit Hilfe des IP Control Protocol (IPCP). Das IPX Control Protocol (IPXCP) regelt parallel die Übermittlung von IPX-Paketen. Zum anderen kann PPP seinerseits über IP oder IPX übertragen werden. Speziell beim Einsatz der im Folgenden beschriebenen Tunnelprotokolle für PPP kommt dieses Verfahren häufig zur Anwendung.

› PAP

Das PPP Authentication Protocol (PAP, RFC 1334 (http://www.ietf.org/rfc/rfc1334.txt)) beschreibt ein Zwei-Wege-Handshake. Das bedeutet, dass der anrufende Knoten die "username/password"-Kombination versendet, um eine Bestätigung von der Gegenstelle zu erhalten. Dies wiederholt er so lange, bis der Kommunikationspartner die Authentifizierung bestätigt oder ablehnt. Im Falle der Ablehnung wird die Verbindung abgebrochen.



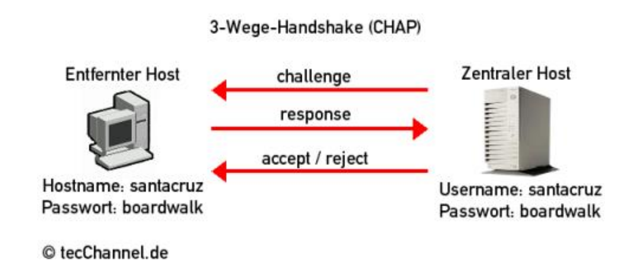
Zwei Wege: Die weit gehende Handlungsfreiheit des Client macht PAP zum potenziellen DoS-Tool.

Dabei ergeben sich eine ganze Reihe von Sicherheitsrisiken:

- Das Passwort wird unverschlüsselt übertragen.
- Der anrufende Knoten kann beliebig viele Versuche unternehmen, sich zu authentifizieren. Dies ermöglicht das Raten von Passwörtern.
- Die Häufigkeit und die Geschwindigkeit der Versuche werden vom anrufenden Knoten bestimmt. Wenn ein oder mehrere Knoten gleichzeitig sehr häufig anrufen (Brute-Force-Attack), kann der zentrale Knoten in seiner eigentlichen Funktion lahmgelegt werden.

› CHAP

Um die bei PAP auftretenden Sicherheitsrisiken zu verringern, wurde das PPP Challenge Handshake Authentication Protocol (CHAP, RFC 1994 (http://www.ietf.org/rfc/rfc1994.txt)) entwickelt.



Drei Wege: CHAP verhindert Brute-Force-Attacken und ermöglicht eine periodische Re-Authentifizierung während der Verbindung.

Es unterscheidet sich von PAP durch eine Reihe zusätzlicher Maßnahmen:

- Häufigkeit und Geschwindigkeit der Authentifizierungsversuche werden im Rahmen eines Drei-Wege-Handshake vom angerufenen Knoten bestimmt, der ein Challenge (eine Herausforderung) an den anrufenden Knoten sendet.
- Die Kombination "username/password" wird per MD-5 verschlüsselt.
- Die Authentifizierung wird nicht nur beim Verbindungsaufbau, sondern auch periodisch während der Verbindung überprüft.

› MS-CHAP v2

Microsoft hat eine eigene Variante eines Authentifizierungsprotokolls für PPTP auf den Markt gebracht, die als Microsoft Challenge Handshake Authentication Protocol version (MS-CHAP) bezeichnet wird. Nachdem die ursprüngliche Version signifikante Sicherheitslücken aufwies, liegt es nunmehr in der zweiten Version als MS-CHAP v2 vor.

Auch MS-CHAP v2 arbeitet nach einem Drei-Wege-Handshake:

- Der Server, zum Beispiel ein Remote-Access-Server, sendet eine Nachricht an den anrufenden Client, die aus einem Session Identifier und einem pseudozufälligen

Challenge String (Client Challenge String) besteht.

- Die Antwort des Client enthält den User-Namen, einen pseudozufälligen Challenge String für den Server (Peer Challenge String), einen Session Identifier sowie einen SHA-1-Hash über den Peer Challenge String, den Session Identifier und das Benutzer-Passwort.
- Der Server antwortet mit der Bestätigung oder Verweigerung der Anmeldung sowie einem SHA1-Hash über Client und Peer Challenge String, die verschlüsselte Antwort des Client und das MD-4-gehashte Passwort.
- Der Client überprüft die Angaben des Servers und nutzt bei erfolgreicher Anmeldung die Verbindung. Ist die Anmeldung nicht korrekt, beendet der Client die Verbindung.

› Vorteile

Gegenüber dem herkömmlichen CHAP weist MS-CHAP v2 eine Reihe von Vorteilen auf:

- Es unterstützt eine wechselseitige Authentifizierung.
- Die Schlüssel werden sowohl vom Benutzerpasswort als auch vom jeweiligen Challenge String abgeleitet. Auf diese Weise verwendet jede Verbindung einen unterschiedlichen Schlüssel.
- Es lassen sich in Hin- und Rückrichtung unterschiedliche Schlüssel verwenden.

MS-CHAP v2 wird während der LCP-Phase beim PPP-Verbindungsaufbau ausgehandelt. Hierfür wird das Feld "LCP Option" auf Typ 3 gesetzt, das Authentifizierungsprotokoll erhält den Wert 0xC223 und der Algorithmus den Wert 0x81. Nach der erfolgreichen Beendigung der LCP-Phase nutzt MS-CHAP v2 das PPP-Protokoll 0xC223.

› ECP

RFC 1968 (http://www.ietf.org/rfc/rfc1968.txt?number=1968) beschreibt mit dem PPP Encryption Control Protocol (ECP) ein Verfahren zum Aushandeln von Verschlüsselungseinstellungen für PPP-Verbindungen. Nach der Konfiguration der Übertragungsparameter via LCP stimmen die Verbindungspartner über identische Nachrichtenformate die Algorithmen und die Schlüssellängen für die aktuelle Sitzung ab.

Den Algorithmen wurden von der IANA (http://www.iana.org/) eindeutige Bezeichner zugeordnet (http://www.iana.org/assignments/ppp-numbers) . Ähnlich dem SSL-Handshake führt der Empfänger der verschlüsselten Nachrichten eine nach seinen Präferenzen geordnete Liste der von ihm unterstützten Algorithmen, die er dem Sender in einer Configure-Request-Nachricht übermittelt. Der Sender wählt aus der Liste die für ihn am besten geeignete Option.

› Tunnelprotokolle

Historisch haben sich drei wichtige Tunnelprotokolle für PPP entwickelt. Hierbei handelt es sich um:

- das Point-to-Point Tunneling Protocol (PPTP),
- das Layer 2 Forwarding (L2F) und
- das Layer 2 Tunneling Protocol (L2TP), das sich nunmehr als Kernprotokoll aus PPTP und L2F herauskristallisiert hat.

Da die Entwicklungen noch vergleichsweise neu sind, finden sich noch alle drei Protokolle in verschiedenen Implementierungen im Einsatz.

› PPTP und L2F

Das Point-to-Point Tunneling Protocol (PPTP) wurde seit 1996 von Ascend Comm, US

Robotics, 3Com, Microsoft und ECI Telematics unter Koordination durch das PPTP-Forum entwickelt. Es eignet sich für den Transfer von IP, IPX oder NetBEUIüber ein IP-Netzwerk.

PPTP verpackt die PPP-Rahmen vor der Übermittlung in IP-Pakete mit der Generic Routing Encapsulation (GRE, RFC 2784 (http://www.ietf.org/rfc/rfc2784.txt)) und sendet sie über ein IP-Netzwerk zum Zielknoten. GRE stellt dabei ähnlich wie TCP Sequenz- und Bestätigungsnummern sowie Mechanismen zur Flusssteuerung (über ein Sliding Window) bereit.

PPTP baut auf dem Remote Access Server für Microsoft Windows NT auf. Auch die Authentifizierung findet auf dem NT-Server statt. Durch die weite Verbreitung von Windows-9x-Clients spielt PPTP beim Aufbau von VPNs noch immer eine gewichtige Rolle. Es verwendet RC4-Verschlüsselung, die Microsoft auch als Microsoft Point-to-Point Encryption (MPPE) bezeichnet.

Das Layer2-Forwarding (L2F) wurde zunächst als proprietäre Entwicklung von Cisco bereitgestellt, aber auch recht bald von Nortel und Shiva unterstützt. Bereits im Mai 1998 als RFC 2341 (http://www.ietf.org/rfc/rfc2341.txt) verabschiedet, wird es mittlerweile aber nur noch der Kategorie "Historic" zugeordnet. L2F wurde für Tunnel von PPP- oder SLIP-Paketen vor der physischen Übertragung entwickelt.

› L2TP

Das Layer2 Tunneling Protocol (L2TP) wurde vom PPTP-Forum und Cisco in Zusammenarbeit mit der IETF (http://www.ietf.org/) im August 1999 verabschiedet und liegt als RFC2661 (http://www.ietf.org/rfc/rfc2661.txt) vor.

Es eignet sich für den Transfer von IP, IPX oder NetBEUIüber ein beliebiges Medium, das die Übertragung von Punkt-zu-Punkt-Datagrammen erlaubt. Hier sind zum Beispiel IP, X.25, Frame Relay oder ATM zu nennen. L2TP fasst PPTP mit L2F zusammen und beschreibt ein umfassendes Vorgehen.

Während PPTP nur Tunnel definiert, die vom Client initiiert werden, und L2F nur Tunnel erlaubt, die vom ISP veranlasst werden, ermöglicht L2TP beide Varianten. Darüber hinaus unterstützt L2TP auch die simultane Verbindung zu mehreren Adressen sowie mehrere sichere Connections.

› Architektur

Der L2TP-RFC verwendet eine Reihe von spezifischen Begriffen zur Beschreibung einer Systemarchitektur:

- LAC: Der L2TP Access Concentrator bildet den einen Endpunkt des L2TP-Tunnels. Wenn der LAC unmittelbar auf dem Client-Rechner läuft, dann spricht man von einem LAC-Client. Der LAC kann aber auch beim ISP implementiert sein.
- LNS: Der L2TP Network Server bildet den anderen Endpunkt des L2TP-Tunnels.
- NAS: Unter einem Network Access Server versteht man ein Gerät, das einen temporären Zugang für Remote-Systeme zur Verfügung stellt. Ein NAS kann gemeinsam mit einem LAC oder einer LNS implementiert sein.

Durch den L2TP-Tunnel wird ermöglicht, dass die normalerweise am Einwahlknoten des ISP endende PPP-Verbindung bis zum Übergang zwischen Internet und Unternehmensnetzwerk erweitert wird.

› Ablauf der L2TP-Connection

Der Verbindungsaufbau über L2TP läuft in insgesamt acht grundlegenden Schritten ab:

- Der Remote-User initiiert eine PPP-Verbindung.
- Der NAS akzeptiert den Ruf.

› Der NAS identifiziert den Remote-User unter Rückgriff auf seinen Authentifizierungsserver.

› Ist die Authentifizierung erfolgreich, initiiert der NAS/LAC einen L2TP-Tunnel zum angestrebten LNS am Zugang zum Zielnetz.

› Der LNS authentifiziert den Remote-User unter Rückgriff auf seinen Authentifizierungsserver.

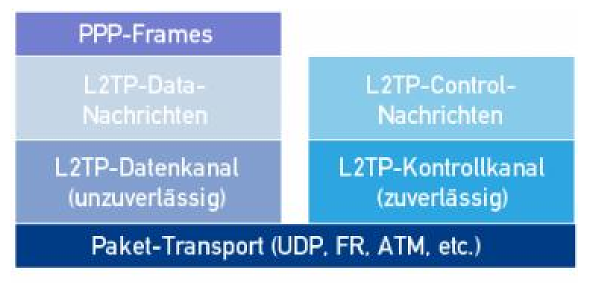
› War die Authentifizierung erfolgreich, bestätigt der LNS den Ruf und den L2TP-Tunnel.

› Der LNS baut die PPP-Verbindung mit dem Remote-User auf.

› Zwischen Remote-User und LNS können nun Datenpakete über die PPP-Verbindung versendet werden.

› Tunnel und Paketformat

Es bestehen verschiedene Möglichkeiten, L2TP in den TCP-IP-Schichtaufbau zu integrieren. Den Ausgangspunkt bilden typischerweise PPP-Pakete, die eine Vielzahl von anderen Protokolldaten führen können. Diese PPP-Pakete werden nun ihrerseits in L2TP-Pakete getunnelt. Die L2TP-Pakete wiederum greifen auf einen Paketdienst zurück. RFC 2661 nennt hier Frame Relay, ATM oder auch UDPüber Port 1701 als Beispiele. UDP wird seinerseits wieder über IP und, wenn es sich um eine serielle oder eine Dial-up-Verbindung handelt, auch wieder über PPP übertragen.



Protokollstruktur: L2TP kennt sowohl Daten- als auch Kontrollpakete.

Natürlich stellt auch L2TP einen klassischen Header zur Verfügung. Dabei ist hervorzuheben, dass L2TP neben den Datenpaketen auch Steuerpakete versendet. Sie sind mit einem identischen Header ausgestattet; lediglich das "Type Field" unterscheidet zwischen Datenpaketen (Typ 0) und Steuerpaketen (Typ 1).



L2TP-Headers: Der Unterschied zwischen Daten- und Kontrollpaketen lässt sich lediglich am ersten Bit erkennen.

L2TP setzt selbst keine Authentifizierungs-, Integritäts- oder Verschlüsselungsmechanismen zum Schutz der getunnelten Pakete auf. Stattdessen verweist der RFC in diesem Punkt auf den IPsec-Standard. Da normale IP-Datagramme den L2TP-Tunnel umschließen, können die IPsec-Header (AH, ESP, IKE) problemlos zum Einsatz kommen. In VPN-Lösungen kommt daher meist eine Kombination aus L2TP und IPsec zum Einsatz.

› AAA

Remote Access Server (RAS) ermöglichen den Dial-in-Zugang in Firmennetze. Deren Bedeutung hat in den vergangenen Jahren erheblich zugenommen.

Entsprechend zugenommen haben auch die Anforderungen an die Sicherheitskonzepte, die sich unter dem Akronym AAA zusammenfassen lassen. Das Kürzel steht für die Begriffe Authentication, Authorization und Accounting.

Als wichtigste Vertreter einer geschlossenen Lösung sind hier RADIUS und TACACS zu nennen. Zu den modernen Erweiterungen zählen insbesondere EAP und IEEE 802.1x.

› RADIUS

Gerade in größeren Installationen ist die zentrale Pflege von Benutzerkennungen, Passwörtern und Zugriffsrechten unabdingbar. Der Remote Authentication Dial-In User Service (RADIUS) wurde speziell für den Nachrichtenaustausch zwischen RAS und einem Server, der alle Benutzerdaten zentral verwaltet, entwickelt.

Der ursprüngliche Entwurf stammt von der Firma Livingston Enterprises, die später von Lucent Technologies übernommen wurde, und basiert auf Vorarbeiten der IETF Network Access Working Requirements Group. Eine IETF-Arbeitsgruppe für RADIUS wurde im Januar 1996 gegründet. Sie bereitete die Verabschiedung der RFCs 2058 (http://www.ietf.org/rfc/rfc2058.txt) und 2138 (http://www.ietf.org/rfc/rfc2138.txt) vor, die später durch RFC 2865 (http://www.ietf.org/rfc/rfc2865.txt) und RFC 2866 (http://www.ietf.org/rfc/rfc2866.txt) ergänzt wurden.

Das RADIUS-Protokoll unterstützt eine Vielzahl von Mechanismen zur Authentifizierung einwählender Benutzer und ist offen für neue Entwicklungen. Die typische Authentifizierung läuft in folgenden Schritten ab:

- Der mobile Client wählt sich beim RAS ein.
- Der RAS formuliert aus den Angaben des Benutzers eine Authentifizierungsanfrage, die verschlüsselt an den RADIUS-Server übermittelt wird.
- Entsprechend der IP-Adresse wählt der RADIUS-Server den richtigen Schlüssel aus einer Datenbank aus und dekodiert das Passwort. Wird ein Eintrag für die Anmeldung gefunden, übermittelt der RADIUS-Server das entschlüsselte Passwort an einen Authentifizierungsserver.
- Sind die Daten korrekt, schickt der RADIUS-Server eine Bestätigung an den RAS und übermittelt zusätzliche Informationen zur Verbindung.
- Diese werden vom RAS an den mobilen Client weitergeleitet.

Ein weiteres typisches Einsatzszenario ist die Authentifizierung in Wireless LANs (http://www.tecchannel.de/hardware/928/10.html) .

› TACACS

Das Terminal Access Controller Access Control System (TACACS) wurde als RFC 1492 (http://www.ietf.org/rfc/rfc1492.txt) standardisiert. Es liegt zusätzlich in zwei von Cisco erarbeiteten Erweiterungen vor: Extended TACACS (XTACACS) und TACACS+.

TACACS ähnelt der Architektur von RADIUS dahingehend, dass ein Remote Client eine Authentifizierungsanfrage an einen Network Access Server stellt, die dieser an einen zentralen Sicherheitsserver (TACACS-Server) weiterleitet. TACACS+ erlaubt wie RADIUS den Einsatz eines separaten Access-Servers, des TACACS+-Servers.

› EAP und 802.1X

Das Extensible Authentication Protocol (EAP, RFC 2284 (http://www.ietf.org/rfc/rfc2284.txt)) stellt eine wichtige Grundlage für eine umfassende und zentralisierte Sicherheitskonzeption dar. Ursprünglich wurde EAP als zuverlässige Authentifizierung der Remote-Access-User für PPP-Links entwickelt. Als allgemeines Protokoll bietet EAP mehrere Authentifizierungsmöglichkeiten. Die Auswahl des Verfahrens findet erst nach dem Link-Aufbau in der Authentifizierungsphase statt.

Von PPP ausgehend hat EAP mittlerweile auch Zugang in das 2001 verabschiedete

IEEE 802.1x gefunden. Ziel dieses Standards ist die Port-bezogene Zugangskontrolle in Netzwerken (Port-based Network Access Control). Die Idee hinter 802.1x besteht darin, einem physischen Anschluss zwei logische Ports zuzuordnen. Der physische Anschluss leitet die empfangenen Pakete grundsätzlich an den so genannten freien Port (Uncontrolled Port) weiter. Der kontrollierte Port (Controlled Port) kann jedoch nur nach einer Authentifizierung erreicht werden. Diese erfolgt über den freien Port.

Die EAP-Messages werden dazu in 802.1x-Nachrichten verpackt (EAP over LAN, EAPOL). In der Regel übernimmt ein RADIUS-Server die Rolle des Authentifizierungsservers. Die EAP-Message wird dann als Attribut im RADIUS-Protokoll übertragen.

› Lücken von 802.1x

IEEE 802.1x stellt eine wichtige Weiterentwicklung im Sicherheitskonzept für Netzwerke dar. Es weist jedoch zwei wesentliche Einschränkungen auf, die vor allem in drahtlosen Netzen zum Tragen kommen:

- Das Verfahren sieht ausschließlich eine Authentifizierung des Client vor, indem der Zugangsserver den Verkehr über den kontrollierten Port erst nach erfolgreicher Authentifizierung freigibt. Dies öffnet den Weg für einen Angriff eines "falschen Servers", den so genannten Man-in-the-Middle-Attack.
- Die einzelnen Pakete enthalten keine Zuordnung mehr. Auf dieser Grundlage kann im Rahmen eines so genannten Session Hijacking ein Angriff dahingehend erfolgen, dass eine WLAN-Station dem erfolgreich authentifizierten Client eine Disassociate-Meldung sendet, die diesen zur Beendigung der Verbindung auffordert. Der Access Point behält aber den kontrollierten Port weiterhin offen, so dass der Angreifer einen Zugang zum Netzwerk erhalten kann.

Solche Angriffe erscheinen bei einer Dial-up-Verbindung nicht praktikabel, da dort durch die Wahl der Telefonnummer der angerufene Partner nicht mehr authentifiziert werden muss. Bei festverdrahteten und entsprechend nach außen abgesicherten festverdrahteten Netzwerken hält sich das Risiko ebenfalls in Grenzen.

› Ausblick

Im vorliegenden Teil unserer Reihe haben wir die Sicherheitsprotokolle auf der Verbindungsschicht des OSI-Modells besprochen. Der nächste Teil wird sich den Sicherheitsmechanismen auf der Netzwerkebene widmen. Dort kommen neben Filterprotokollen, die als Access Control Lists implementiert werden, vor allem Verschlüsselung (wie IPsec) sowie Masquerading-Protokolle zum Einsatz. Der Schwerpunkt des nächsten Kapitels unserer Reihe liegt aber auf der Darstellung der außerordentlich unübersichtlichen IPsec-Standardfamilie. (jlu)

Grundlagen: Security

Teil 1	Einführung in die Kryptographie
Teil 2	Kryptologische Verfahren
Teil 3	Security auf dem Link Layer
Teil 4	Security auf dem Network Layer
Teil 5	Security auf dem Application Layer
Teil 6	Security mit VPNs

› Weitere Themen zu diesem Artikel:

Security im Überblick (Teil 1) (http://www.tecchannel.de/software/1068/index.html)
Security im Überblick (Teil 2) (http://www.tecchannel.de/software/1095/index.html)
Security im Überblick (Teil 4) (http://www.tecchannel.de/software/1168/index.html)
Security im Überblick (Teil 5) (http://www.tecchannel.de/software/1194/index.html)
Sicherheit im WLAN (http://www.tecchannel.de/hardware/928/index.html)
Public-Key-Infrastrukturen (http://www.tecchannel.de/software/1113/index.html)
Webdienste und Sicherheit (http://www.tecchannel.de/software/1088/index.html)

Security im Überblick (Teil 4)

› Zu den beliebtesten Sicherheitsverfahren auf der Netzwerkschicht zählt IPsec. Wir erläutern das Zusammenspiel der IPsec-Protokollfamilie und nehmen zudem IP-Masquerading näher unter die Lupe.

› VON AXEL SIKORA

Auf der Netzwerkebene können verschiedene Protokolle eingesetzt werden, um die Sicherheit bei der Anbindung an das öffentliche Internet zu erhöhen. Dazu zählen:

- › Encryption-Protokolle, wobei IPsec von besonderem Interesse, aber leider auch von besonderer Komplexität ist
- › Filter-Protokolle, die als Access Control Lists implementiert werden,
- › und Umsetzungsprotokolle, die ein Verstecken von Rechnern (Masquerading) ermöglichen.

Da die beiden letzten Typen eng miteinander verbunden sind und oft in einem Gerät implementiert werden, erläutern wir sie hier zusammen. Der Schwerpunkt dieses Teils unserer Reihe liegt aber auf der Darstellung der außerordentlich unübersichtlichen IPsec-Standardfamilie.

Grundlagen: Security

Teil 1	Einführung in die Kryptographie
Teil 2	Kryptologische Verfahren
Teil 3	Security auf dem Link Layer
Teil 4	Security auf dem Network Layer
Teil 5	Security auf dem Application Layer
Teil 6	Security mit VPNs

› IPsec

IPsec wird in den IETF-Standards RFC2401 ff beschrieben. Es handelt sich dabei um ein Verfahren zur Verschlüsselung, Integrität und Authentifizierung sicherheitsrelevanter Daten auf der Netzwerkschicht. IPsec versucht, allen Teilnehmern und denkbaren Anwendungsszenarios gerecht zu werden, was eine ungeheure Vielzahl von Kombinationen auf allen Stufen ermöglicht.

Zusätzlich ist noch der Aufbau der RFCs, deren unmittelbare Bestandteile die unten stehende Tabelle zeigt, so unübersichtlich, dass ein eigener RFC2410 (http://ietf.org/rfc/rfc2410.txt) deren gegenseitige Abhängigkeiten beschreibt. Darüber hinaus gibt es noch weitere RFCs, die durch IPsec betroffen sind und zum Teil obsolet wurden, sowie mehrere RFCs, welche die in den IPsec-RFCs verwendeten kryptographischen Verfahren definieren.

RFCs zur IPsec-Protokollfamilie

Titel	RFC
Security Architecture for the Internet Protocol	RFC 2401
IP Authentication Header	RFC 2402
The Use of HMAC-MD5-96 within ESP and AH	RFC 2403

The Use of HMAC-SHA-1-96 within ESP and AH	RFC 2404
The ESP DES-CBC Cipher Algorithm with Explicit IV	RFC 2405
IP Encapsulation Security Payload (ESP)	RFC 2406
The Internet IP Security Domain of Interpretation for ISAKMP	RFC 2407
Internet Security Association and Key Management Protocol (ISAKMP)	RFC 2408
The Internet Key Exchange (IKE)	RFC 2409
The NULL Encryption Algorithm and It5s Use With IPsec	RFC 2410
IP Security Document Roadmap	RFC 2411
The Oakley Key Determination Protocol	RFC 2412

› IPsec-Struktur

Durch seine unübersichtliche Struktur widerspricht IPsec vollkommen dem Grundsatz, die Architektur sicherer Systeme so einfach wie möglich zu gestalten. Dennoch erfreut es sich einer großen Beliebtheit bei der Implementierung von Virtuellen Privaten Netzwerken (VPN). Die Komplexität von IPsec ist aber ein wesentlicher Grund dafür, dass insbesondere die VPN-Produkte auf der Netzwerkschicht oftmals in proprietären Produkten angeboten werden.

IPsec umfasst zwei große Funktionsgruppen: die Übertragungsprotokolle sowie das Schlüsselmanagement. Zum Datentransfer dienen Verfahren wie Authentication Header (AH, RFC2402 (http://ietf.org/rfc/rfc2402.txt)) und Encapsulation Security Payload (ESP, RFC2403 (http://ietf.org/rfc/rfc2403.txt)).

Die Verwaltung der Schlüssel beschreiben die eng zusammenhängenden Funktionen Internet Security Association and Key Management Protocol (ISAKMP, RFC 2408 (http://ietf.org/rfc/rfc2408.txt)), Internet Key Exchange (IKE, RFC 2409 (http://ietf.org/rfc/rfc2409.txt)) sowie Domain of Interpretation (DOI, RFC2407 (http://ietf.org/rfc/rfc2407.txt)).

› Security Association

Der Realisierung von IPsec liegt das Konzept der Security Association (SA) zu Grunde. Unter einer Security Association versteht man eine kryptographisch geschützte Verbindung. Die SA wird vom Protokoll-Stack je Kommunikationspartner und verwendetem Protokoll eingerichtet. Das heißt, dass für eine bidirektionale Verbindung zwischen zwei Kommunikationspartnern mindestens zwei SA aufgebaut werden müssen.

Eine SA wird für IPsec eindeutig beschrieben durch das Tripel: (SPI, IP-Zieladresse, Security Protocol). Beim Security Parameter Index (SPI) handelt es sich um eine 32-Bit-Zahl, die der Empfänger beim Aufbau der SA willkürlich auswählt. Das ermöglicht, in Kombination mit der IP-Adresse des Empfängers jedes empfangene Paket mit einem IPsec-Header eindeutig einer SA zuzuordnen. Falls ein IPsec-Paket mit IP-Multicast-Adresse als Empfänger und einem vergebenen SPI eintrifft, kann es zurückgewiesen werden. Der Eintrag für das Security Protocol beschreibt das Übertragungsverfahren, beispielsweise AH oder ESP.

› Security Association Database

Anhand des Tripels lässt sich die SA als Index in der Security Association Database (SAD) verwalten. Dazu werden zu jeder geschützten Netzwerkverbindung folgende sicherheitsrelevante Konfigurationsdaten gespeichert:

- › IPsec-Dienst (AH oder ESP)
- › Übertragungsmodus (Transport vs. Tunnel Modus)
- › Authentifikations- und Verschlüsselungsalgorithmus

› Schlüssel

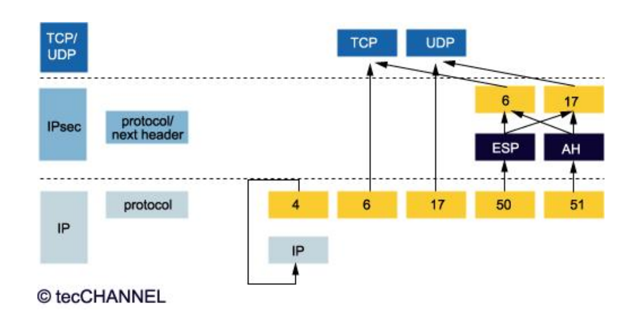
› Sequenznummer

› Angaben zur Lebensdauer der SA

Der gesamte Datenverkehr auf einem IPsec-System richtet sich nach Sicherheitsregeln, die in einer weiteren Datenbank, der Security Policy Database (SPD) definiert werden. Die Regeln legen - unter anderem über die Einträge von Absender- und Zieladresse, Absender- und Zielport sowie Protokoll (TCP/UDP) - fest, welche Verbindungen mit Sicherheitsfunktionen versehen werden. Die SPD wertet diese Liste ähnlich aus wie eine Firewall ihre Regelbasis: Alle Einträge werden sequenziell untersucht. Trifft keines der Selektionskriterien zu, kann IPsec das Paket nicht bearbeiten.

› Protokoll-Auswahl

IPsec arbeitet zwischen IP und TCP/UDP, wobei es in der Regel der Netzwerkschicht zugeordnet wird. Unsere Abbildung zeigt die grundsätzliche Architektur sowie die Zuordnung der Protokoll- und Portnummern.



Zahlenspiele: IPsec identifiziert den Aufbau eintreffender Pakete anhand der Protokollfelder im Header.

Die Abbildung ist folgendermaßen zu lesen:

› Enthält das Protokollfeld eines IP-Headers die Zahl 6, dann handelt es sich um ein TCP-Paket.

› Enthält das Protokollfeld eines IP-Headers die Zahl 50, dann folgt dem IP-Header ein ESP-Header, es findet eine Übertragung nach IPsec-ESP statt.

› Enthält das Protokollfeld des IPsec-Headers die Zahl 6, dann folgt ein TCP-Header.

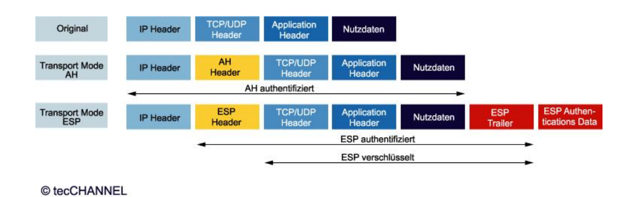
Zusätzlich sind die Spezialfälle des Tunnelns zu berücksichtigen:

› Enthält das Protokollfeld eines IP-Headers die Zahl 4, dann enthält das IP-Paket wiederum ein IP-Paket.

› Enthält das Protokollfeld des IPsec-Headers mit dem Typ AH die Zahl 51, dann folgt dem IPsec-Header ein ESP-Header.

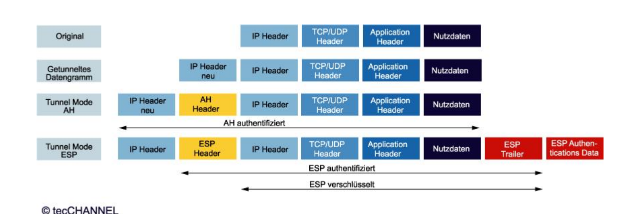
› IPsec-Modi

IPsec unterscheidet zwei grundsätzliche Übertragungsmodi. Der Transport-Modus fügt zusätzliche IPsec-Informationen zwischen IP-Header und Datenpaket ein und erlaubt einen günstigen Einsatz bei der sicheren Ende-zu-Ende-Kommunikation.



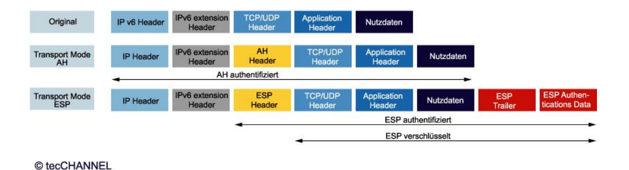
Transport Mode: Die einfachere Übertragungsvariante von IPsec beschränkt den Header-Overhead.

Der Tunnel-Modus ergänzt einen kompletten IP-Header und IPsec-Informationen (Abbildung 6). Er wird dann benötigt, wenn die originalen IP-Quell- und Zieladressen unbedingt beibehalten werden sollen. Damit findet der Tunnel-Modus Anwendung in Firewall-to-Firewall, bzw. Firewall-to-End-Kommunikation.



Tunnel Mode: Der Tunnel-Modus von IPsec kapselt alle Informationen komplett in ein neues IP-Paket.

Dazu ist anzumerken, dass man beim Entwurf von IPsec durchaus auf den Transport-Modus hätte verzichten können. Sein einziger Vorteil besteht darin, dass man sich beim Transfer den zusätzlichen IP-Header spart. Angesichts der hohen Komplexität von IPsec bei der Realisierung in den Endpunkten erscheint dieser Vorteil allerdings nur marginal.

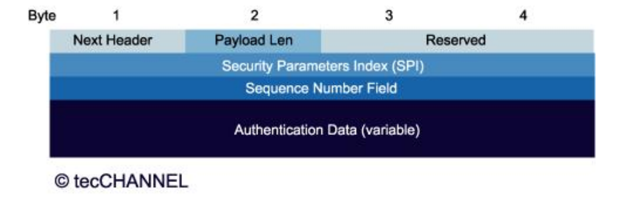


IPsec und IPv6: Die AH- und ESP-Header werden hier wie alle anderen Extension Header abgearbeitet.

Oft findet man die Anmerkung, das IPsec bereits in IPv6 integriert sei. Das betrifft aber nicht - wie manchmal fälschlicherweise impliziert wird - die Authentifizierung oder der Verschlüsselung, sondern lediglich das Konzept der Extension Header. Die obige Abbildung zeigt, wie sich AH- und ESP-Header in die Reihe der anderen möglichen IPv6-Extension-Header einfügen.

› Authentication Header (AH)

Das Übertragungsverfahren mit Hilfe des Authentication Header (AH) beschreibt RFC2402 (http://ietf.org/rfc/rfc2402.txt) . AH gewährt eine verbindungslose Integrität sowie die Authentifizierung eines IP-Pakets und erlaubt den Schutz gegen so genannte Replay-Angriffe. Die Absicherung schließt auch die IP-Header ein, mit Ausnahme allerdings solcher Felder, die von den Routern auf dem Weg eines Pakets durch ein IP-Netz verändert werden (mutuable fields).



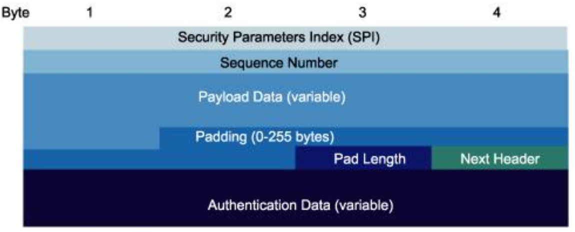
AH-Struktur: Der Authentication Header garantiert Integrität und Authentizität der Header-Daten.

Das Next-Header-Feld gibt Auskunft über das dem AH-Header folgende Protokoll (etwa 6 für TCP). Payload Len beschreibt die Länge des AH in 32 Bit-Wörtern. Auf das derzeit noch nicht genutzte Reserved-Feld folgt der schon besprochene Security Parameter Index (SPI). Die Sequence Number identifiziert die Reihenfolge des Paketes in der Kommunikation. Pakete mit doppelten oder nicht plausiblen Sequenznummer verwirft IPsec, was einfacher Replay-Angriffe unterbindet

Das Feld Authentication Data beinhaltet die kryptographische Prüfsumme, die nach dem in der SA definierten Algorithmus berechnet wurde. Dabei kommen entweder HMAC-MD5 oder HMAC-SHA-1 zum Einsatz. Deren Verwendung mit AH und ESP beschreiben RFC2403 (http://ietf.org/rfc/rfc2403.txt) (HMAC-MD5-96) und RFC2404 (http://ietf.org/rfc/rfc2404.txt) (HMAC-SHA-1-96). Eine Reihe von Implementierungen verwendet MD5/SHA-1 nur mit der Keyed-Variante. Dann erfolgt ein Hashing nur mit dem Shared Key, was lediglich eine Integritätskontrolle ermöglicht. Bei der HMAC-Variante (Hashed Message Authentication Code) wird das Keyed-Ergebnis zusätzlich mit dem Secret Key (Integrität und Authentifizierung) verarbeitet.

› Encapsulating Security Payload (ESP)

Die Übertragung mittels Encapsulating Security Payload (ESP) beschreibt RFC2406 (http://ietf.org/rfc/rfc2406.txt) , das den originalen RFC1827 ablöst. ESP erlaubt über die Mechanismen des AH hinaus auch eine Verschlüsselung des Datenpakets. Hierfür ist ESP etwas komplexer aufgebaut als AH. Insbesondere verwendet ESP nicht nur einen eigenen Header, sondern hängt auch einen Trailer an.



Daten-Klammer: ESP umschließt die Nutzdaten mit einem eigenen Header und Trailer.

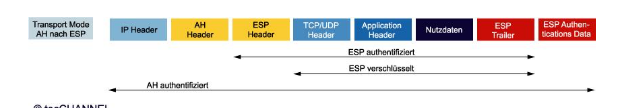
Der ESP-Header besitzt die in der obigen Abbildung gezeigten Bestandteile. Security Parameter Index (SPI) und Sequence Number kennen wir bereits aus der Beschreibung des AH. Die Nutzdaten (Payload Data) transferiert ESP üblicherweise verschlüsselt. Dazu nutzt es den DES-Algorithmus im CBC-Modus (RFC2405 (http://ietf.org/rfc/rfc2405.txt)). Alternativ lassen sich die Daten auch ohne Verschlüsselung übermitteln. Die sogenannte Null Encryption beschreibt der humorige RFC2410 (http://ietf.org/rfc/rfc2410.txt) .

Die Authentifizierung (Authentication Data) erfolgt ebenfalls verschlüsselt. Dazu nutzt ESP wahlweise HMAC-MD5 (RFC2403 (http://ietf.org/rfc/rfc2403.txt)) oder HMAC-SHA-1 (RFC2404 (http://ietf.org/rfc/rfc2404.txt)). Optional kann auch hier eine Null Authentication zum Einsatz kommen. Jedoch dürfen nicht gleichzeitig Nutzlast und Authentifizierung unverschlüsselt übermittelt werden.

› AH/ESP-Kombinationen

AH und ESP lassen sich nicht nur einzeln einsetzen, sondern dürfen auch kombiniert werden. Grundsätzlich unterscheidet man zwei Kombinationsverfahren:

- › Transport Adjacency: Beide Sicherheitsprotokolle werden im Transport-Modus auf das gleiche IP-Datagramm angewendet.
- › Nested Tunneling: Beide Sicherheitsprotokolle arbeiten im Tunnel-Modus zusammen. Da das Tunneling jeweils wieder ein neues IP-Datagramm zusammenstellt, lassen sich hier die beiden Protokolle theoretisch beliebig oft anwenden.



Transport Adjacency: Jede IPsec-Implementation muss für den Transport Mode diese sehr sichere AH/ESP-Kombination implementieren.

Auf den unterschiedlichen Stufen einer Übertragung dürfen beide Varianten ihrerseits wiederum kombiniert werden. So ergibt sich eine schier endlose Zahl von Varianten. RFC2406 (http://ietf.org/rfc/rfc2406.txt) beschreibt deswegen verpflichtende Kombinationen, die jede IPsec-Implementierung abdecken muss:

- Der Transport-Modus muss AH allein, ESP allein sowie AH nach ESP (im Sinn der Transport Adjacency) unterstützen.
- Der Tunnel-Modus muss sowohl AH allein als auch ESP allein implementieren.

Weitere Kombinationen können optional realisiert werden, was allerdings zu Lasten der Interoperabilität geht: Eine lediglich standardkonforme Gegenstation ist nicht verpflichtet, zusätzliche Varianten ebenfalls zu unterstützen.

› Schlüsselmanagement

Die AH- und ESP-RFCs beschreiben lediglich die IPsec-Übertragungsverfahren. Sie treffen jedoch keine Aussage darüber, wie die gemeinsamen Schlüssel und deren Sicherheitsparameter in der Security Association Database zwischen den Kommunikationspartnern ausgehandelt werden. Hier existieren (wie stets bei IPsec) zwei Möglichkeiten: Eine manuelle Verteilung und Konfiguration sowie ein automatisierter Verwaltungsmechanismus.

Kleinere, dedizierte Applikationen wählen auf Grund der relativ hohen Komplexität der automatisierten Protokolle recht häufig den manuellen Ansatz. Um das automatisierte Verfahren zu beschreiben, gilt es zunächst die Begriffe ISAKMP, DOI und IKE zu klären:

- Das Internet Security Association and Key Management Protocol (ISAKMP, RFC2408) bildet eine Rahmenarchitektur für die Verwaltung von Security Associations (SA) und Schlüsseln. Darüber hinaus beschreibt es auch die Organisation der Datenpakete zum Generieren von Schlüsseln und der Authentifizierungsdaten. ISAKMP selbst stellt aber kein Protokoll zum Schlüsselaustausch dar. Es ist auch keineswegs nur auf den Einsatz mit IPsec beschränkt, sondern für die Verwaltung von beliebig strukturierten SAs ausgelegt.
- Die Domain of Interpretations (DOI, RFC2409) beschreiben verschiedene Protokolle, die mit ISAKMP verwendet werden können. In Bezug auf die Verwendung in IPsec instanziiert DOI ISAKMP für die Verwendung bei IP.
- Bei Internet Key Exchange (IKE, RFC2409) handelt es sich um ein Protokoll zum Austausch von Schlüsseln und zur Verwaltung von SAs für die AH- und ESP-Protokolle von IPsec. Hierzu nutzt IKE Bestandteile sowohl von ISAKMP als auch von Oakley (RFC2412), das ein Diffie-Hellman-Schlüsselaustauschverfahren beschreibt.

› ISAKMP

IKE besteht aus zwei Stufen. In der ersten Phase finden eine wechselweise Authentifizierung und das Aushandeln eines langfristigen Sitzungsschlüssels statt. Dazu handeln die miteinander kommunizierenden Systeme eine Security Association für die sichere Übertragung von ISAKMP-Nachrichten aus. Darauf aufbauend können in der zweiten Phase beliebig viele SAs für IPsec-Verbindungen oder andere Protokolle über IKE möglichst effizient aufgebaut werden.

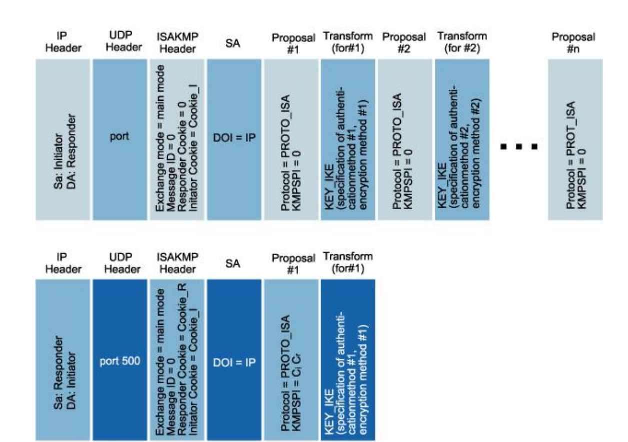
Für den gegenwärtig in der Praxis üblichen Fall, dass nur zwei SAs ausgehandelt werden müssen, wirkt sich diese Aufteilung eher nachteilig aus und kompliziert den Ablauf unnötig. Hinzu kommt, dass in der Phase 1 zwischen zwei Modi und in der Phase 2

zwischen drei Modi ausgewählt werden kann.

Für die Phase 1 muss die Implementation den Main Mode unterstützen, der sechs Datagramme austauscht. Optional lässt sich der Aggressive Mode mit einem vereinfachten Austausch von nur drei Datengrammen realisieren. Darüber hinaus gilt es noch zu unterscheiden, auf welche Weise die Schlüssel generiert und ausgetauscht werden sollen. Hier existieren die Varianten pre-shared secret key, public-encryption key (alias public signature key) sowie original public key-encryption.

› ISAKMP Phase 1

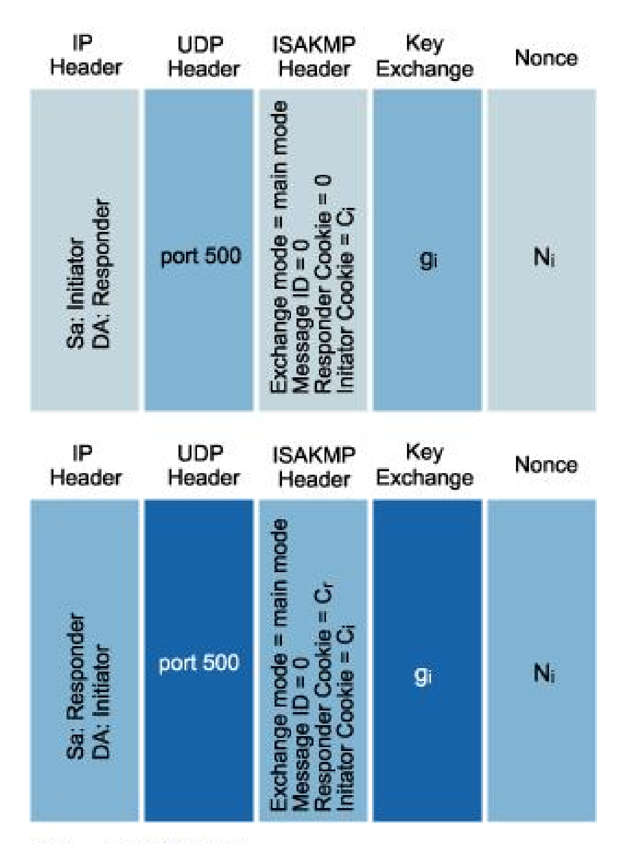
Die folgenden Grafiken zeigen schematisch den Ablauf von Phase 1 einer ISAKMP-Verhandlung.



Erste Kontaktaufnahme: Der Initiator konfrontiert in Message 1 (oben) den Responder mit diversen Vorschlägen über die zu nutzenden Algorithmen. In Message 2 (unten) wählt der Responder die ihm geeignet erscheinenden aus.

Message 1: Der Initiator konfrontiert den Responder mit einer Auswahl von verschiedenen Vorschlägen (Proposals), nach welchen Verschlüsselungs- und Authentifizierungsalgorithmen (Transform) die ISAKMP-SA ausgehandelt werden könnte. Im ISAKMP-Header wird das Feld Initiator-Cookie auf einen Pseudozufallswert C(i) gesetzt, der dann später zusammen mit dem Responder-Cookie C(r) den Nachrichtenfluss authentifiziert. Nachrichten innerhalb eines ISAKMP-Paketes können sich in langen Folgen aneinander reihen. Dabei gibt jede Nachricht über das Feld Next Payload an, ob noch weitere Nachrichten folgen. Dabei können mehrere Transform-Nachrichten zu einer Proposal-Nachricht und mehrere Proposal-Transform-Kombinationen zu einer SA gehören.

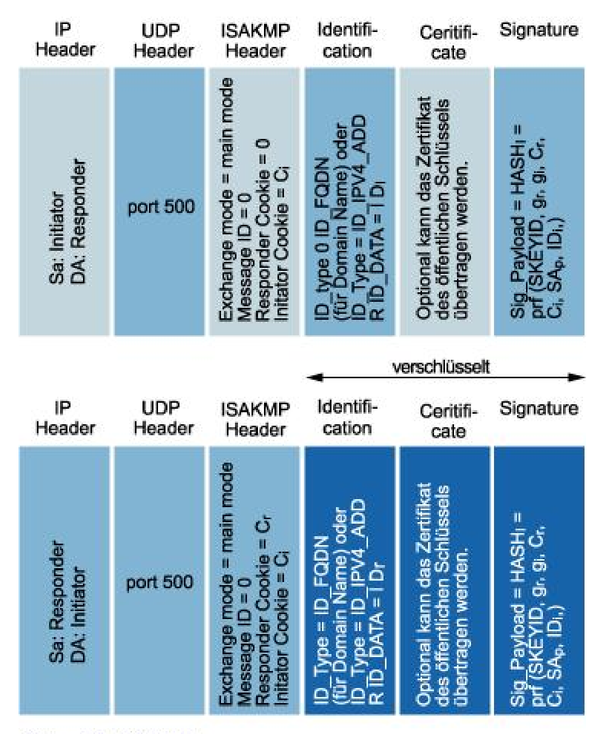
Message 2: Der Responder antwortet, indem er sich aus den Vorschlägen einen heraussucht. Das Rahmenformat ist identisch mit der Message 1. Im ISAKMP-Header setzt der Responder das Feld Responder-Cookie auf einen Pseudozufallswert C(r). Zusätzlich repliziert er auch C(i), so dass eine erste (schwache) Authentifizierung stattfindet. C(r) und C(i) bilden zusammen als SPI den Index für den Zugriff auf die Security Association Database mit den gemeinsamen Verbindungsparametern.



Kryptographische Verhandlung: In Message 3 (oben) und 4 (unten) tauschen Initiator und Responder Informationen zur Schlüsselgenerierung aus.

Message 3: Mit der dritten Nachricht beginnt nun der Austausch der kryptographischen Informationen. Der Initiator teilt seinen öffentlichen Diffie-Hellman-Schlüssel g(i) mit. Zudem liefert er eine pseudozufällige und große Zahl, die man als Nonce (engl. für Ad-hoc) N(i) bezeichnet.

Message 4: Der Responder antwortet mit seinem öffentlichen Diffie-Hellman-Schlüssel g(r) und seiner Nonce N(r). Aus diesen Informationen berechnen nun beide Stationen eine Reihe von unterschiedlichen Schlüsseln. Hierzu zählt insbesondere der Master-Key SKEYID. Aus diesem werden verschiedene weitere Schlüssel abgeleitet, die zur Verschlüsselung beim nachfolgenden Datentransfer zum Einsatz kommen. SKEYID_d ist der Schlüssel, der in der zweiten IKE-Phase zur Verschlüsselung von nicht-ISAKMP-konformen SAs eingesetzt wird. SKEYID_a wird zur Authentifizierung von ISAKMP-Nachrichten verwendet, SKEYID_e zur deren Verschlüsselung.



Letzter Check: Die benötigten Schlüssel sind jetzt generiert. In Message 5 (oben) und 6 (unten) prüfen die Kommunikationspartner die Verbindung mit einem ersten, verschlüsselten Transfer.

Nun haben beide Stationen die für die Übertragung benötigten Schlüssel generiert und überprüfen diesen Status mit den beiden letzten Nachrichten Message 5 und Message 6. Hierbei übertragen sie eine verschlüsselte Authentifizierung.

› ISAKMP Phase 2

Der Aggressive Mode verkürzt die Phase 1 auf nur drei Nachrichtentransfers. Der Initiator schickt im ersten Paket neben dem vorgeschlagenen Verfahren auch gleich seinen öffentlichen Diffie-Hellman-Schlüssel mit. Dem Responder bleibt nichts anderes übrig, als das Angebot anzunehmen oder zu verwerfen.

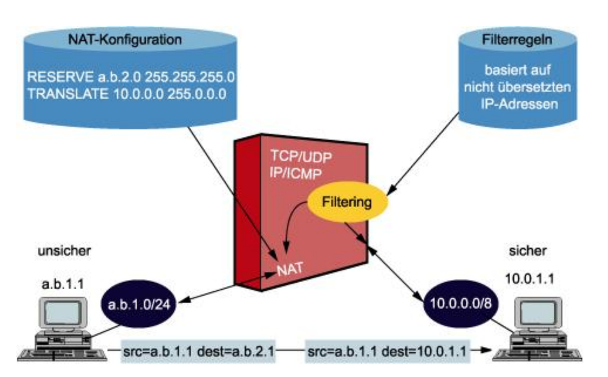
Auf der Grundlage der gesicherten Kommunikation zur Übermittlung von ISAKMP-Nachrichten können nun Initiator und Responder in Phase 2 beginnen, beliebig viele SAs für IPsec-Verbindungen einzurichten. Dazu tauschen sie im so genannten Quick Mode Exchange drei Nachrichten, die sie allesamt mit dem in Phase 1 generierten Schlüssel SKEYID_e chiffrieren. Außerdem versehen sie die Nachrichten mit einer kryptographischen Prüfsumme, in deren Berechnung SKEYID_a eingeht.

Im ersten Schritt schlägt der Initiator wieder mögliche Algorithmen zur Einrichtung einer oder mehrerer SAs sowie deren Verwendungszweck vor. Die Gegenstelle trifft eine Auswahl und übermittelt diese mit der zweiten Nachricht. Neben Main-, Aggressive- und Quick-Mode definiert IKE noch zwei weitere Exchanges:

- › Der Informational Exchange dient zum Übermitteln von Status- und Fehlerinformationen sowie Löschen von SAs.
- › Mit dem New Group Exchange kann ein neuer Diffie-Hellman-Modus für die ISAKMP-SA ausgehandelt werden.

› IP Masquerading

Neben IPsec zählt IP-Masquerading zu den bekanntesten Sicherheitsmechanismen auf der Netzwerkschicht. Das auch als IP Network Address Translation (NAT) bezeichnete Verfahren wird in RFC3022 (http://ietf.org/rfc/rfc3022.txt) beschrieben.



NAT im Überblick: Die Außenkommunikation aller Clients im lokalen Netz wird über eine einzelne Public-IP-Adresse abgewickelt. Dabei ergeben sich zusätzliche Filterungsmöglichkeiten.

NAT erlaubt eine transparente Umsetzung zwischen den internen Adressen eines LAN und der Adresszuordnung im öffentlichen Netz. Ursprünglich wurde es entwickelt, um zusätzliche Hosts ans Internet anschließen zu können, ohne dafür knappe öffentliche IPv4-Adressen nutzen zu müssen. Mittlerweile hat es sich aber auch zum Sicherheits-Feature speziell für kleinere LANs entwickelt, die nicht über weitergehende Sicherheitsmechanismen wie SOCKS- oder Proxy-Server verfügen.

NAT schafft eine Zuordnung zwischen (in der Regel privaten) IP-Adressen in einem sicheren Netz und einer IP-Adresse im unsicheren, öffentlichen Netz. Dem gemäß ist NAT immer in einem Router implementiert. Aus der Außensicht treten alle internen Rechner im Internet so auf, als würden sie alle die gleiche, öffentliche IP-Adresse verwenden.

› Sicherheitsaspekte

Bei der Adressumsetzung via NAT ergeben sich eine Reihe von interessanten Aspekten:

- › NAT beschreibt keinen Tunnelmechanismus. Es wird also kein zusätzlicher IP-Header angehängt, sondern der bestehende IP-Header modifiziert. Dieses Verfahren arbeitet prinzipiell sehr effizient, da es keine zusätzlichen Daten generiert. Allerdings bringt es bei einigen Applikationen, die auch auf Anwendungsebene IP-Adressen berücksichtigen, Probleme mit sich.
- › Sind mehrere interne IP-Adressen auf eine externe IP-Adresse abzubilden, wie dies bei typischen Dial-up-Routern der Fall ist, dann muss die Umsetzungstabelle noch zusätzliche Informationen abspeichern. Anhand der verwendeten Source-TCP-Ports bleibt eine eindeutige Zuordnung möglich. Dies bedeutet aber einen deutlich höheren Verwaltungsaufwand für den NAT-Router, der die Zuordnung verbindungsorientiert treffen muss.
- › Im gleichen Schritt kann auch die Entscheidung fallen, ein Paket mit einer bestimmten Zieladresse (outbound) oder Quelladresse (inbound) gar nicht umzusetzen, sondern statt dessen zu blockieren. Diese Filterung auf Adressebene kann als IP-Firewall verstanden werden. Auf der Basis der entsprechenden Cisco-Nomenklatur hat sich dafür auch der Begriff der Access-Control-Lists durchgesetzt.

› Ausblick

Im vorigen und im aktuellen Teil unserer Artikelserie zu Security haben wir uns näher mit den grundlegenden Sicherheitsverfahren auf den beiden untersten Schichten des Netzwerks vertraut gemacht. Davon ausgehend nehmen wir im nächsten Teil der Serie die wichtigsten Sicherheitsprotokolle auf der Anwendungsschicht des Netzwerks näher unter die Lupe.

Zu deren bekanntesten Vertretern zählen SSL/TLS und das darauf basierende HTTPS. Daneben kommen auch eigenständige Protokolle wie S/MIME und S/HTTP sowie das

Lieblingswerkzeug des Administrators, SSH, zur Sprache. (jlu (http://www.tecchannel.de/impressum/jluther.html))

Grundlagen: Security

Teil 1	Einführung in die Kryptographie
Teil 2	Kryptologische Verfahren
Teil 3	Security auf dem Link Layer
Teil 4	Security auf dem Network Layer
Teil 5	Security auf dem Application Layer
Teil 6	Security mit VPNs

› Weitere Themen zu diesem Artikel:

- Security im Überblick (Teil 1) (http://www.tecchannel.de/software/1068/index.html)
- Security im Überblick (Teil 2) (http://www.tecchannel.de/software/1095/index.html)
- Security im Überblick (Teil 3) (http://www.tecchannel.de/software/1144/index.html)
- Security im Überblick (Teil5) (http://www.tecchannel.de/software/1194/index.html)
- Workshop: VPN mit Linux (http://www.tecchannel.de/betriebssysteme/897/index.html)
- Firewall-Grundlagen (http://www.tecchannel.de/special/977/index.html)
- Kryptographie-Grundlagen (http://www.tecchannel.de/internet/416/index.html)
- So funktionieren TCP/IP und IPv6 (http://www.tecchannel.de/internet/209/index.html)

Security im Überblick (Teil 5)

› Auf der Transport- und Anwendungsschicht finden sich die populärsten Sicherheitsmechanismen für Netzwerke. Dazu zählen SSL/TLS und S-HTTP, Proxys und Firewalls sowie RADIUS und Kerberos.

› VON AXEL SIKORA

Auch auf den Transport- und Anwendungsebenen des Netzwerks existieren vielfältige Konzepte, um eine sichere Kommunikation über unsichere Verbindungen zu ermöglichen. Hierzu zählen insbesondere:

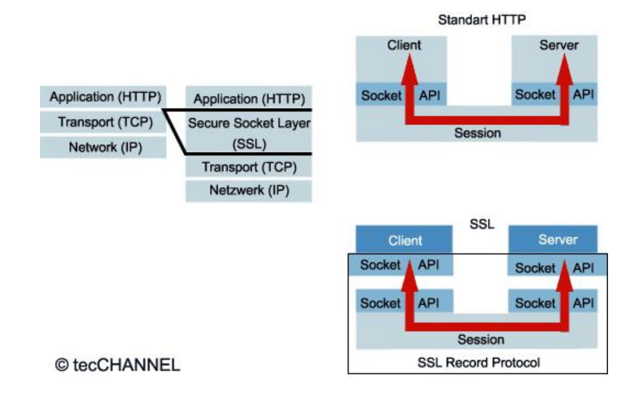
- › Verschlüsselungs- und Authentifizierungsmechanismen,
- › Firewalls und Proxys sowie
- › Systeme zur Authentifizierung.

Grundlagen: Security

Teil 1	Einführung in die Kryptographie
Teil 2	Kryptologische Verfahren
Teil 3	Security auf dem Link Layer
Teil 4	Security auf dem Network Layer
Teil 5	Security auf dem Application Layer
Teil 6	Security mit VPNs

› Transportprotokolle

Bei dem seit 1994 gemeinsam von Netscape und RSA Security entwickelten Secure-Socket-Layer-Protokoll (SSL) handelt es sich um das wohl bekannteste Sicherheitsprotokoll auf Transportebene.



Transparent: SSL legt ein eigenes Socket-API zwischen die Anwendung und die TCP-Sockets.

Ziel ist die Bereitstellung eines privaten Kanals zwischen Kommunikationsanwendungen, um Vertraulichkeit und Integrität der Daten sowie die Authentifizierung der Partner zu gewährleisten. Hierzu implementiert SSL den RSA-Algorithmus für das Management des Sitzungsschlüssels sowie einen symmetrischen Algorithmus (etwa DES oder RC4) zur Verschlüsselung der Nutzdaten.

SSL stellt ein alternatives TCP/IP-Socket-API zur Verfügung, das über inhärente

Sicherheitsmerkmale verfügt und seinerseits auf die normalen TCP-Sockets zugreift. Auf diese Weise können prinzipiell alle Anwendungen, die normalerweise über TCP/IP kommunizieren, ihre Daten auch über SSL austauschen.

› SSL / TLS

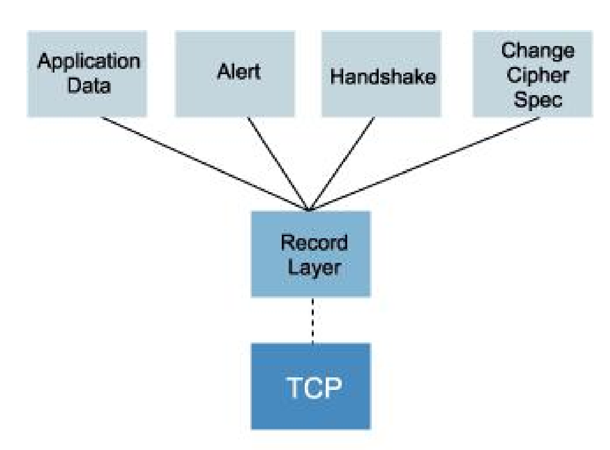
In der Praxis hat sich vor allem der Einsatz von HTTP über SSL durchgesetzt. Die URL für einen SSL-basierten HTTP-Zugriff beginnt meist mit https:. Im Unterschied zu S-HTTP ist HTTPS dabei kein eigenes Protokoll, hier erfolgt lediglich der HTTP-Zugriff über SSL. Daneben existieren auch Erweiterungen, mit denen sich FTP, SMTP oder NNTPüber SSL absetzen lassen. SSL setzt eine zuverlässige Übertragung auf der Transportebene voraus, so dass in der Regel der Einsatz von TCP gewählt wird.

Im Mai 1996 gründete die IETF eine Arbeitsgruppe Transport Layer Security (TLS), um ein an SSL angelehntes Protokoll zu standardisieren. Ziel war die Harmonisierung der Ansätze von Netscape (SSLv3) und Microsoft (STLP). Nach langen Diskussionen und Wirren konnte im Januar 1999 TLS als RFC 2246 (http://www.ietf.org/rfc/rfc2246.txt) verabschiedet werden. TLS und SSLv3 sind in fast allen Bereichen identisch. Viele Werkzeuge, einschließlich des Microsoft Internet Explorer, unterstützen TLS. Der Netscape Navigator bleibt jedoch bislang außen vor.

SSL liegt in einer Reihe von offenen Implementierungen vor. Insbesondere sind die Bibliotheken von OpenSSL (http://www.openssl.org/) zu nennen, die alle notwendigen Routinen zum Erstellen eigener Programme und Werkzeuge zur Generierung asymmetrischer Schlüssel und X.509-Zertifikate beinhalten.

› SSL-Verbindungsaufbau

Bei SSL handelt es sich um ein verbindungsorientiertes Protokoll. Damit gliedert sich jede Kommunikation in die drei Phasen Verbindungsaufbau, Datenübertragung und Verbindungsabbau. Für den Verbindungsaufbau wird ein mehrstufiger Handshake-Prozess definiert.



Mehrstufig: Beim SSL-Handshake werden mehrere Nachrichtenarten über einen einheitlichen Record Layer übertragen.

Das Handshake dient sowohl zur Authentifizierung des Servers als auch für das Aushandeln der Schlüssel, die bei der nachfolgenden verschlüsselten Datenübertragung eingesetzt werden sollen. SSL besteht dabei aus einer Reihe von verschiedenen Nachrichtenarten, die mit Hilfe eines einheitlichen Record Layer übertragen werden.

› Ablauf

Ein typischer SSL-Verbindungsaufbau läuft in folgenden Schritten ab:

- GET HTTPS://: Der Client ruft ein SSL-geschütztes Dokument auf dem Server auf, gekennzeichnet durch eine URL mit dem Protokollbezeichner HTTPS://.

- › Handshake HelloRequest: Der Server sendet hierauf einen Hello-Request an den Client, der den eigentlichen SSL-Handshake startet.
- › Handshake ClientHello: Der Client sendet dem Server eine Liste von unterstützten Algorithmen sowie eine Zufallszahl für die Erzeugung des Schlüssels. SSL und TLS unterstützen eine Vielzahl von Verschlüsselungsverfahren unterschiedlicher Qualität und Komplexität.
- › Handshake ServerHello: Der Server sucht einen Algorithmus aus den vom Client angebotenen Verfahren aus und informiert den Client hierüber.
- › Handshake Certificate: Der Server sendet seinen öffentlichen RSA-Schlüssel in einem gültigen X.509-Zertifikat an den Client.
- › Handshake ServerHelloDone: Zusätzlich versendet auch der Server eine Zufallszahl, die ebenfalls für die Erzeugung des Schlüssels benötigt wird.
- › Handshake ClientKeyExchange: Der Client überprüft das Zertifikat des Servers. Dann erzeugt er eine zufällige Zeichenfolge (pre_master_secret) und sendet diese verschlüsselt zum Server. Auf der Grundlage der beiden von Server und Client erzeugten Zufallszahlen und des pre_master_secret berechnen Client und Server unabhängig voneinander die Schlüssel für Verschlüsselung und die Signaturen (MAC).
- › ChangeCipherSpec: Der Client informiert dann den Server, dass alle weiteren Pakete verschlüsselt übertragen werden.
- › Handshake Finished: Das Finished-Paket enthält ein MAC über alle Handshake-Nachrichten an den Server. So findet der Server heraus, ob ein Man-in-the-Middle-Angriff die originalen Pakete des Client verändert hat.
- › ChangeCipherSpec: Der Server informiert den Client, dass alle weiteren Pakete verschlüsselt übertragen werden.
- › Handshake Finished: Auch das Finished-Paket des Servers enthält ein MAC über alle Handshake-Nachrichten an den Server. So kann auch der Client herausfinden, ob ein Man-in-the-Middle-Angriff die originalen Pakete des Servers verändert hat.

Damit ist die SSL-Verbindung aufgebaut, und die verschlüsselte Datenübertragung kann beginnen.

› Anwendungsprotokolle

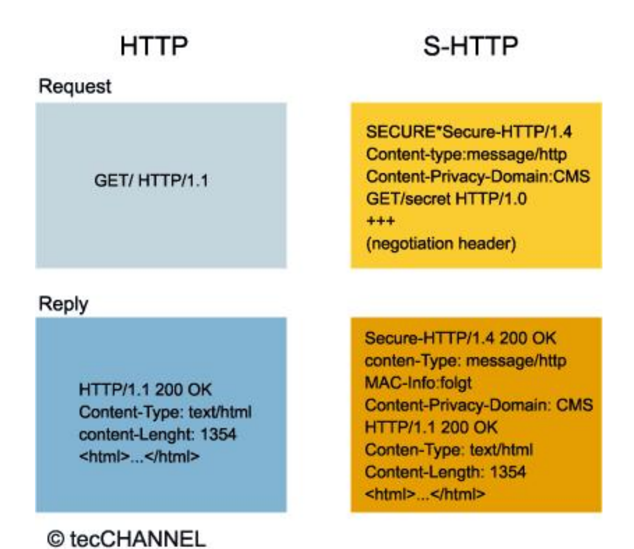
Komplementär zu HTTP via SSL steht mit Secure HTTP auch eine zweite Syntax zur sicheren Übertragung von HTTP-Paketen zur Verfügung. S-HTTP behandelt und schützt dabei jede HTTP-Nachricht einzeln.

Wie viele andere der hier vorgestellten Sicherheitsprotokolle bietet S-HTTP sowohl Befehle zum Aushandeln der Sicherheitsparameter ("negotiation format") als auch zur Übertragung der gesicherten Daten ("message format").

Das Nachrichtenformat von S-HTTP basiert auf der Cryptographic Message Syntax (CMS), die in RFC 2630 (http://www.ietf.org/rfc/rfc2630.txt) beschrieben ist. CMS ist eine Variante der PKCS #7 (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/) , die für S/MIME entwickelt wurde. Auf beide gehen wir im Folgenden noch ein.

› S-HTTP

S-HTTP-Pakete weisen das äußere Erscheinungsbild von HTTP-Requests und -Responses auf. Insbesondere nutzt S-HTTP den gleichen TCP-Port wie HTTP, versendet aber CMS-Nachrichten. Um dies dem Server mitzuteilen, wird in S-HTTP mit Secure ein spezieller Request-Typ definiert, der dem eigentlichen HTTP-Header vorangestellt wird.



HTTP vs. S-HTTP: Secure HTTP sichert alle HTTP-Daten komplett ab.

Den prinzipiellen Aufbau im Vergleich zu konventionellem HTTP-Verkehr zeigt die obige Abbildung. Im Rahmen der S-HTTP-Verhandlung steht eine Vielzahl von verschiedenen Möglichkeiten zur Verfügung. Generell lassen sich eine digitale Signatur ("sign"), eine Verschlüsselung des Inhalts ("encrypt") und die symmetrische Authentifizierung des Inhalts ("auth") auswählen, wobei jeweils ein ganzer Satz von Parametern zur Anwendung kommt.

› SSH

Ein Shell-Account bietet vollen Zugriff auf das Dateisystem und alle Funktionen des Rechners. Die früher dafür verwendeten Programme Telnet (über Port 23/tcp) beziehungsweise rlogin/rsh sind jedoch prinzipiell unsicher, da sie das Passwort im Klartext übertragen.

Mit SSH beziehungsweise Secure Shell bezeichnet man sowohl ein kryptographisches Protokoll als auch eine konkrete Implementierung dieses Protokolls. Ursprünglicher Designer des SSH-Protokolls und Autor der zugehörigen Software ist Tatu Ylönen aus Finnland. Er entwickelte die Secure Shell an der TU Helsinki und gründete später die Firma SSH Communications Security (http://www.ssh.com/) .

Zum Funktionsumfang von Ylönens Secure Shell gehören:

- › das Login auf einer entfernten Maschine,
- › die interaktive oder nicht interaktive Ausführung von Kommandos auf der entfernten Maschine sowie
- › das Kopieren von Dateien zwischen verschiedenen Rechnern eines Netzes.

› SSH1 vs. SSH2

SSH ermöglicht eine kryptographisch gesicherte Kommunikation über unsichere Netze und bietet ein hohes Sicherheitsniveau, zuverlässige gegenseitige Authentifizierung der Partner sowie Integrität und Vertraulichkeit der ausgetauschten Daten. SSH definiert sowohl die Verschlüsselung des gesamten Datenverkehrs als auch passwortbasierte oder Public/Private-Key-Login-Methoden ohne Einsatz von Klartext.

Unterschiede zwischen SSH1 und SSH2

SSH Version 1	SSH Version 2
Blowfish	TripleDES
DES	RC4

TripleDES	Twofish
RC4	

Gegenwärtig existieren zwei unterschiedliche und inkompatible Versionen des SSH-Protokolls: SSH 1.x und SSH 2.x. Das SSH-Protokoll 1.x ist nicht international standardisiert und mit einigen konzeptionellen Mängeln behaftet, die durch die Version 2.x behoben werden. SSH 2.x wird durch Internet Drafts der Secure Shell Working Group (http://www.ietf.org/html.charters/secsh-charter.html) der IETF beschrieben.

› SSH-Implementationen

Der SSH-Server läuft standardmäßig auf Port 22/tcp. Mittels Portweiterleitung (Port Forwarding) lässt sich über SSH aber auch anderer Verkehr abwickeln. So kann beispielsweise ein POP3-Client seinen Verkehr auf den lokalen SSH-Port umleiten, damit über diesen die Daten an den POP3-Server durch einen so genannten SSH-Tunnel transportiert werden.

Die in ANSI-C geschriebene, unter UNIX lauffähige SSH 1.0 wurde von Tatu Ylönen im Juni 1995 freigegeben. Bis zur Version 1.2.12 war Ylönens Software zu beliebigen Zwecken frei nutzbar, später wurden die Lizenzbedingungen restriktiver. Daher basiert beispielsweise die völlig freie OpenSSH auf der SSH 1.2.12.

Ylönens Firma SSH Communications Security beteiligt sich aktiv an der Weiterentwicklung der SSH und bietet Implementierungen des Protokolls 2.x als Produkte an, die unter bestimmten Bedingungen kostenfrei (http://www.ssh.com/support/downloads/) genutzt werden dürfen. Neben dieser "offiziellen" SSH-Variante gibt es eine ganze Reihe anderer Implementierungen unterschiedlicher Qualität, die zum Teil völlig unabhängig davon entstanden sind.

› OpenSSH und OSSH

Mit OpenSSH und OSSH stehen zwei kostenfrei nutzbare, in C geschriebene SSH-Implementierungen für Unix zur Verfügung. Sie wurden und werden ausgehend von Tatu Ylönens Quellen der SSH 1.2.12 entwickelt und wiesen gegenüber dem Original eine ganze Reihe von Erweiterungen und Verbesserungen auf. Im Gegensatz zu Ylönens SSH unterstützen OpenSSH und SSH die beiden symmetrischen Chiffren IDEA und DES nicht.

Bei OpenSSH (http://www.openssh.com/) handelt es sich um eine Entwicklung des OpenBSD-Projekts und gehört ab dessen Version 2.6 zum Standardumfang. OpenSSH wird aktiv gepflegt und beherrscht ab Version 2.1.0 zusätzlich zum SSH-Protokoll 1.x auch das Protokoll 2.0. OSSH (ftp://ftp.pdc.kth.se/pub/krypto/ossh/) wird von Björn Grönvall entwickelt und steht ebenfalls für eine Vielzahl von Unix-Systemen zur Verfügung.

Auch für Windows existieren SSH-Implementationen. Zu deren bekanntesten zählt die Freeware putty (http://www.chiark.greenend.org/~sgtatham/putty) , die über ein grafisches Interface sowohl SSH1 als auch SSH2 zur Verfügung stellt.

› E-Mail-Verkehr

Für die Absicherung von E-Mail-Nachrichten existiert eine Reihe von Security-Mechanismen und Verfahren. In der Praxis haben davon vor allem Pretty Good Privacy (PGP) und Secure MIME (S/MIME) eine größere Verbreitung gefunden.

Kaum eine Rolle spielen dagegen beim Anwender bislang der Privacy Enhanced Mail Standard (PEM, RFC 1421 (http://www.ietf.org/rfc/rfc1421.txt) bis RFC 1424) und die MIME Object Security Services (MOSS, RFC 1847 (http://www.ietf.org/rfc/rfc1847.txt) und RFC 1848 (http://www.ietf.org/rfc/rfc1848.txt)). Dies liegt nicht zuletzt an gewissen funktionalen Einschränkungen der beiden Standards.

› PGP

Das kostenlos erhältliche (http://www.pgp.com/) Pretty Good Privacy (PGP) zählt zu den

meistgenutzten Verschlüsselungsprogrammen im Internet. PGP realisiert hybride Verschlüsselungsverfahren, bei denen neben RSA- und Diffie-Hellman-Algorithmen wahlweise AES, CAST, Triple-DES, IDEA oder TwoFish zum Einsatz kommen.

Ein wesentlicher Grund für die weite Verbreitung von PGP war die Verfügbarkeit mit langen und damit (schon vor der Exportöffnung der USA) sicheren Schlüssellängen. Mittlerweile ist PGP in einer komfortablen grafischen Benutzeroberfläche integriert, die eine Verwendung und Administration einfach gestalten.

Ein wichtiges Merkmal bei der Verwendung öffentlicher Schlüssel ist die Authentifizierung: die Bestätigung also, dass der Schlüssel wirklich vom Absender kommt. Hierzu bietet PGP zusätzlich zur sicheren Übermittlung die Möglichkeit, ein so genanntes Web of Trust aufzubauen. Es basiert darauf, dass bereits als zuverlässig bekannte Kommunikationspartner weitere, jeweils selbst überprüfte Kontakte über ihre Signatur zertifizieren.

PGP unterstützt also sowohl Verschlüsselung ("encryption") als auch Authentifizierung ("signature"). Darüber hinaus komprimiert es den Datenstrom mit Hilfe der als Freeware verfügbaren Kompressionsroutine von Jean-Loup Gailly, Mark Adler und Richard B. Wales, die auch in PKZip 2.x der Firma PKWare eingesetzt wird.

› S/MIME

Secure MIME (S/MIME) Version 2 wurde ursprünglich von den RSA Labs entwickelt und greift auf das verschlüsselte Nachrichtenformat PKCS #7 (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/) zurück. Im Gegensatz zu PGP verwendet S/MIME die weit verbreiteten X.509-Zertifikate.

Da ein solches Zertifikat nur von einer Zertifizierungsstelle beglaubigt werden kann, fallen hier in der Regel Kosten an, was die Verbreitung gegenwärtig noch hemmt, obwohl eine Vielzahl von Mail-Clients S/MIME schon unterstützt.

› Firewalls

Die Hauptaufgabe einer Firewall besteht darin, die Zugriffskontrolle auf das interne Netzwerk zu zentralisieren. Aus technischer Sicht existieren zwei grundlegend verschiedene Konzepte der Firewall-Realisierung: Paketfilter und Proxy-Gateways.

Paketfilter oder Überwachungs-Router (screening router) arbeiten auf der Netzwerk- und Transportschicht und stellen die einfachste Variante einer Firewall dar. Sie werten ein- und ausgehende Datenpakete nach den Header-Informationen in IP-, ICMP-, TCP- oder UDP-Paketen aus. Auf Grund dieser Informationen treffen sie gegebenenfalls die Entscheidung, ein Paket mit einer bestimmten Zieladresse ("outbound") oder Quelladresse ("inbound") zu blockieren.

```
Yosemite(config)# access-list 103 deny tcp
                  10.1.2.1 0.0.0.0
                  10.1.1.0 0.0.0.255
                  eq 80
Yosemite(config)# access-list 103 permit any
Yosemite(config)# interface ethernet 0
Yosemite(config-if)# ip access-group 103 in
```

Simpel: Access Control Lists dienen zur Implementation einfacher Paketfilter.

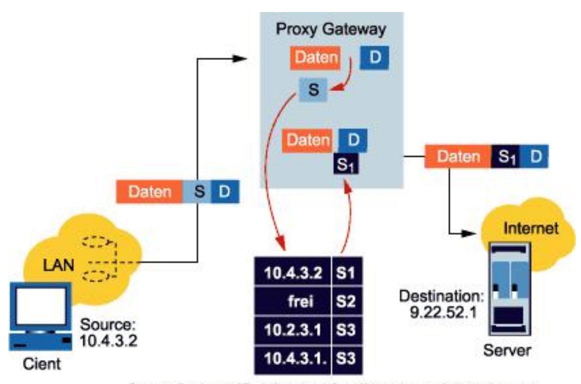
In der Regel sind die Sende- und Empfangsadresse, die Portnummer der Anwendung, TCP-Statusinformationen sowie der Nachrichtentyp bei ICMP-Nachrichten die Grundlage für eine solche Entscheidung. Das vielleicht bekannteste Beispiel hierfür sind die Access Control Lists (ACL), wie sie in Cisco-Routern Einsatz finden. Aber auch die von Linux verwendeten ipchains beziehungsweise iptables erfüllen die gleiche Funktion.

Application Level Gateways arbeiten, wie der Name nahe legt, zusätzlich auf Anwendungsebene und können entsprechend auch anwendungsspezifische Informationen in den Filterprozess miteinbeziehen. Auf diese Weise lassen sich beispielsweise bestimmte Operationen in einzelnen Protokollen sperren. So kann man etwa über das Sperren des PUT-Befehls in FTP den Upload unerwünschter Dateien

verhindern.

› Proxy-Gateways

Proxy-Gateways sind wie Überwachungs-Router dezidierte Rechner, über die alle Verbindungen zwischen dem internen Netz und dem Internet geleitet werden. Im Unterschied zu den Paketfiltern trennen sie jedoch die Verbindungen am Übergang zwischen den Netzen.

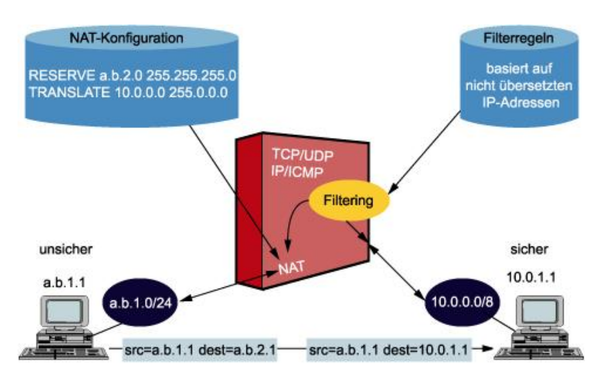


Logische Trennung: Der Proxy führt den Verbindungsaufbau stellvertretend für den internen Rechner aus.

Bei einem Verbindungsaufbau eines internen Client prüft der Gateway zunächst, ob er den adressierten Ziel-Host im Internet kontaktieren und den angeforderten Dienst nutzen darf. Danach führt der Proxy (Englisch: Stellvertreter) den Verbindungsaufbau stellvertretend für den internen Host aus. Der Zielrechner empfängt die Datenpakete mit der Absenderadresse des Proxy, an den er auch seine Antworten zurückschickt. Der Proxy reicht die Daten dann über seine interne Schnittstelle an den anfragenden Client weiter.

› Circuit Level Gateways

Bei Circuit Level Gateways handelt es sich um Proxy-Gateways mit erweiterten Funktionen. Sie haben als anwendungsunabhängige Multiprotokoll-Proxies auf Transportebene die Aufgabe, die Verbindungsdaten zwischen internem und externem Netz zu überwachen und bei erfüllten Regeln weiterzuleiten. Circuit Level Gateways unterscheiden sich von Paketfiltern lediglich darin, dass sie die Verbindung unterbrechen und die intern verwendeten IP-Adressen per Masquerading verbergen können.



NAT im Überblick: Die Außenkommunikation aller Clients im lokalen Netz wird über eine einzelne Public-IP-Adresse abgewickelt. Dabei ergeben sich zusätzliche Filterungsmöglichkeiten.

Unter IP-Masquerading versteht man die IP Network Address Translation (NAT), wie sie in RFC 3022 (http://www.ietf.org/rfc/rfc3022.txt) beschrieben ist. Diese erlaubt die

Adressumsetzung zwischen den internen Adressen eines Netzwerks und der Adresszuordnung im öffentlichen Netz. Ursprünglich wurde NAT entwickelt, um im beschränkten IPv4-Adressraum weitere Hosts anschließen zu können.

Mittlerweile hat sich NAT aber eher zum Sicherheits-Feature insbesondere für kleinere Netze entwickelt, die nicht über weiter gehende Sicherheitsmechanismen wie SOCKS oder Proxy-Server verfügen. Eine genauere Beschreibung (http://www.tecchannel.de/software/1168/13.html) des Verfahrens finden Sie in Teil 4 (http://www.tecchannel.de/software/1168/index.html) dieser Artikelreihe.

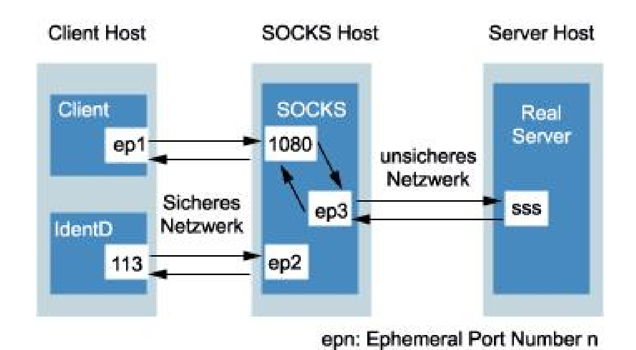
› SOCKS

Damit eine Internet-Anwendung trotz Eingabe der externen Zieladresse zuerst das Gateway kontaktiert, muss oft die Software intern angepasst werden. Alle Socket-Calls der Anwendung sind durch neue Aufrufe zu ersetzen, anschließend muss der Programm-Code neu kompiliert werden. SOCKS ist eine Sammlung von Werkzeugen, die entwickelt wurde, um bestehende Client-/Server-Anwendungen in Proxy-Versionen der gleichen Anwendung umzuwandeln. Die Algorithmen von SOCKS Version 5 (SOCKSv5) sind in RFC 1928 (http://www.ietf.org/rfc/rfc1928.txt) beschrieben.

Dem Anpassungsproblem kann man auch durch den Einsatz zusätzlicher Software begegnen. Das kostenlos erhältliche SocksCap (ftp://) von NEC arbeitet unter allen Windows-Versionen zwischen den Anwendungen und dem TCP/IP-Stack (Winsock). Dort fängt SocksCap alle Aufrufe ab und setzt sie zur Laufzeit in das SOCKS-Protokoll um. Viele Standard-Client- und -Server-Programme besitzen mittlerweile eigene Proxy-Fähigkeiten oder unterstützen generische Proxy-Systeme wie SOCKS. Dies gilt insbesondere für Anwendungen aus dem Unix-/Linux-Umfeld.

› SOCKS v5

Der Verbindungsaufbau unter SOCKSv5 verläuft nach einem Muster, das auch Eingang in den Standard IEEE 802.1x gefunden hat. Hierfür beobachtet der SOCKSv5-Server einen bestimmten Port (meist 1080), an den der Client seine initiale Verbindungsanfrage sendet.



SOCKS v5: Während der Authentifizierungsphase werden Verfahren und Parameter ausgehandelt.

Wenn die Anfrage zugelassen und die Verbindungsanfrage erfolgreich sind, beginnt eine Authentifizierungsphase, bei der der Client nach dem Aushandeln der Authentifizierungsverfahren und -parameter seine Identität nachweisen muss.

› AAA - Authentication, Authorization, Accounting

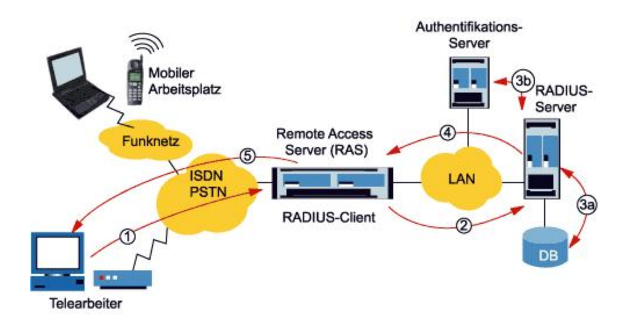
Remote Access Server (RAS) ermöglichen den Dial-in-Zugang in Firmennetze. Deren Bedeutung hat in den vergangenen Jahren erheblich zugenommen.

Entsprechend gestiegen sind damit auch die Anforderungen an die zugehörigen Sicherheitskonzepte, die sich unter dem Akronym AAA (Triple-A - Authentication, Authorization, Accounting) zusammenfassen lassen.

Als wichtigste Vertreter einer geschlossenen Lösung sind hier RADIUS und TACACS zu nennen. Bei den modernen Erweiterungen sind insbesondere EAP und 802.1X hervorzuheben.

› RADIUS

In größeren Installationen ist die zentrale Pflege von Benutzerkennungen, Passwörtern und Zugriffsrechten unverzichtbar. Der Remote Authentication Dial-in User Service (RADIUS) wurde für den Nachrichtenaustausch zwischen RAS und einem Server entwickelt, der alle Benutzerdaten zentral verwaltet.



Architekturschema: Typischer Aufbau einer RADIUS-Installation im Überblick.

Die ursprüngliche Entwicklung stammt von der Firma Livingston Enterprises, die später von Lucent Technologies übernommen wurde. Sie basiert dabei auf Vorarbeiten der IETF Network Access Working Requirements Group. Eine IETF-Arbeitsgruppe für RADIUS wurde im Januar 1996 gegründet. Sie bereitete die Verabschiedung der RFCs 2058 (http://www.ietf.org/rfc/rfc2058.txt) und 2138 (http://www.ietf.org/rfc/rfc2138.txt) vor, die später durch RFC 2865 (http://www.ietf.org/rfc/rfc2865.txt) und RFC 2866 (http://www.ietf.org/rfc/rfc2866.txt) ergänzt wurden.

› Ablauf der RADIUS-Authentifizierung

Das RADIUS-Protokoll unterstützt eine Vielzahl von Mechanismen zur Authentifizierung einwählender Benutzer und ist offen für neue Entwicklungen. Ein typischer Einsatz unter Verwendung eines RAS läuft folgendermaßen ab:

- Der mobile Client wählt sich beim RAS ein.
- Der RAS formuliert aus den Angaben des Benutzers eine Authentifizierungsanfrage (authentication request), die verschlüsselt an den RADIUS-Server übermittelt wird.
- Entsprechend der IP-Adresse wählt der RADIUS-Server den richtigen Schlüssel aus einer Datenbank aus und decodiert das Passwort. Wird ein Eintrag für die Anmeldung gefunden, übermittelt der RADIUS-Server das entschlüsselte Passwort an einen Authentifizierungsserver.
- Sind die Daten korrekt, schickt der RADIUS-Server eine Bestätigung an den RAS und übermittelt zusätzliche Informationen zur Verbindung.
- Diese werden vom RAS an den mobilen Client weitergeleitet.

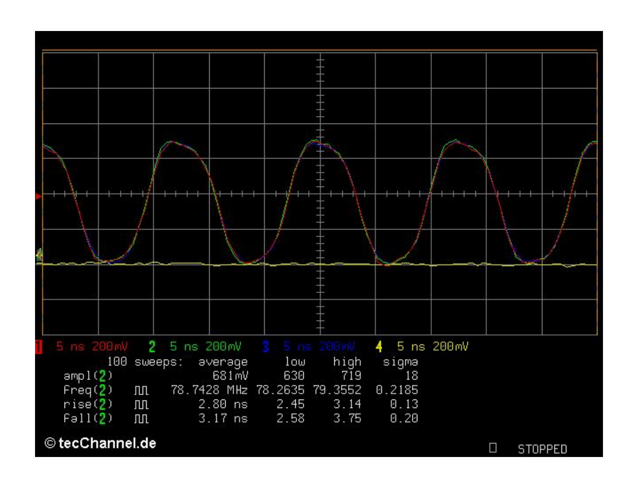
› TACACS

Das Akronym TACACS steht für Terminal Access Controller Access Control System. Das Verfahren wurde als RFC 1492 (http://www.ietf.org/rfc/rfc1492.txt) standardisiert. Es liegt zusätzlich in zwei von Cisco (http://www.cisco.com/) erarbeiteten Erweiterungen (http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:Tacacs_plus) vor: Extended TACACS (XTACACS) und TACACS+.

TACACS ähnelt der Architektur von RADIUS dahingehend, dass ein Remote Client eine Authentifizierungsanfrage an einen RAS-Server stellt, die dieser an einen zentralen Sicherheitsserver (TACACS-Server) weiterleitet. TACACS+ erlaubt wie RADIUS den Einsatz eines separaten Access-Servers, des TACACS+-Servers.

› Kerberos

Der Name des Kerberos-Protokolls beruft sich auf den dreiköpfigen Hund Zerberus, der in der griechischen Mythologie die Pforte der Unterwelt Hades bewacht und der nur von Odysseus und Herakles überwunden wird. Der Kerberos Network Authentication and Authorization Service Version 5 ist in RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt) beschrieben.



Drei Köpfe: Die Kerberos-Architektur arbeitet mit getrennten Authentifizierungs- und Ticketing-Servern sowie einer Datenbank.

Der Kerberos-Dienst wird normalerweise auf einem eigenen System betrieben und stellt ein verschlüsseltes Sicherheitssystem zur wechselseitigen Authentifizierung von Clients und Servern dar. Benutzer müssen sich zunächst bei Kerberos anmelden, bevor sie auf andere Server zugreifen dürfen.

Der Kerberos-Dienst teilt sich in zwei Bestandteile auf: den Kerberos Authentication Server (KAS), der die Authentifizierung durchführt, und den Kerberos Ticket Granting Server (TGS), der den Client mit dem Nachweis ausstattet, dass dieser auf den Dienst eines weiteren Servers im System zugreifen darf.

› EAP und 802.1x

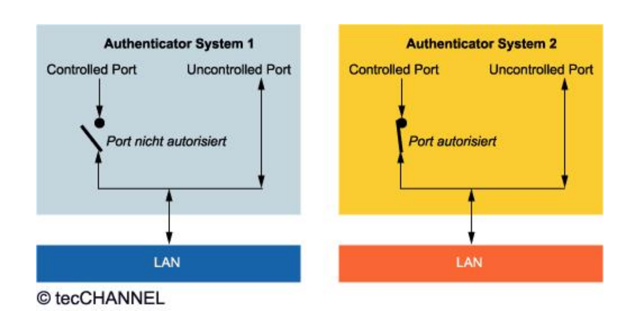
Das Extensible Authentication Protocol (EAP - RFC 2284 (http://www.ietf.org/rfc/rfc2284.txt)) bildet eine wichtige Grundlage für umfassende und zentralisierte Sicherheitskonzepte. Ursprünglich wurde EAP für PPP-Links entwickelt, um eine zuverlässige Authentifizierung für Remote Access User bereitzustellen.

Bei EAP handelt es sich um ein allgemeines Protokoll, das mehrere Authentifizierungsmöglichkeiten bietet. Die Auswahl des Verfahrens findet bei PPP erst nach der Link Control Phase (LCP) in der Authentifizierungsphase statt.

Von PPP ausgehend hat EAP mittlerweile auch Zugang in den im Jahr 2001 verabschiedeten Standard IEEE 802.1x gefunden, der die physische Übertragung für LAN-Netzwerke anpasst. Die EAP-Messages werden hierzu in 802.1x-Nachrichten verpackt (EAP over LAN - EAPOL). Ziel dieses Standards ist die portbezogene Zugangskontrolle in Netzwerke (Port-Based Network Access Control).

› Struktur von 802.1x

Die Idee hinter IEEE 802.1x besteht darin, einem physischen Anschluss zwei logische Anschlüsse (Ports) zuzuordnen. Der physische Anschluss leitet die empfangenen Pakete grundsätzlich an den so genannten freien Port (Uncontrolled Port) weiter.



Zweiteilung: IEEE 802.1x trennt den physischen Anschluss in zwei logische Ports auf.

Der kontrollierte Port (Controlled Port) lässt sich jedoch nur nach einer Authentifizierung erreichen. Diese kann über den freien Port erfolgen (siehe Abbildung). In der Regel übernimmt bei 802.1x ein RADIUS-System die Rolle des Authentifizierungs-Servers. Die EAP-Message wird dann als Attribut im RADIUS-Protokoll übertragen.

› Lücken von IEEE802.1x

Der IEEE-802.1x-Standard stellt eine wichtige Weiterentwicklung im Sicherheitskonzept für Netzwerke dar. Dabei bleiben jedoch zwei wesentliche Aspekte ausgespart:

- IEEE 802.1X sieht eine Authentifizierung des Client nur vor, indem der Access Point den kontrollierten Port erst nach erfolgreicher Authentifizierung freigibt. Der Client selbst befindet sich unmittelbar im authentifizierten Modus. Dies öffnet den Weg für Angriffe von "falschen Servern", so genannten Man-in-the-Middle-Attacken.
- Die einzelnen Pakete enthalten keine Zuordnung mehr. So kann im Rahmen eines so genannten Session Hijacking ein Angriff dahingehend erfolgen, dass eine andere Station dem erfolgreich authentifizierten Client eine Disassociate-Meldung sendet, die diesen zur Beendigung der Verbindung auffordert. Der Access Point hält aber den kontrollierten Port weiterhin offen, so dass der Angreifer darüber Zugang zum Netz erhalten kann.

Allerdings erscheinen solche Angriffe insbesondere bei Dial-up-Verbindungen nicht sonderlich praktikabel: Der Kommunikationspartner lässt sich dort recht zuverlässig über die angerufene Telefonnummer identifizieren. Auch bei festverdrahteten und entsprechend nach außen abgesicherten Netzwerken bleibt das Risiko vergleichsweise gering.

› Ausblick

Mit der Beschreibung der Sicherheitsmechanismen auf Transport- und Anwendungsebene haben wir schon beinahe das Ende unserer Security-Reihe erreicht.

Im nächsten und letzten Teil werden wir uns mit einer Sicherheitstechnologie beschäftigen, die derzeit immer mehr an Bedeutung gewinnt: den Virtual Private Networks (VPNs). Mit Hilfe von VPNs lassen sich externe Rechner über öffentliche Netzwerke sicher an das Unternehmensnetz anbinden. (jlu)

Grundlagen: Security

Teil 1	Einführung in die Kryptographie
Teil 2	Kryptologische Verfahren
Teil 3	Security auf dem Link Layer
Teil 4	Security auf dem Network Layer
Teil 5	Security auf dem Application Layer
Teil 6	Security mit VPNs

› Weitere Themen zu diesem Artikel:

Security im Überblick (Teil 1) (http://www.tecchannel.de/software/1068/index.html)
Security im Überblick (Teil 2) (http://www.tecchannel.de/software/1095/index.html)
Security im Überblick (Teil 3) (http://www.tecchannel.de/software/1144/index.html)
Security im Überblick (Teil 4) (http://www.tecchannel.de/software/1168/index.html)
Firewall-Grundlagen (http://www.tecchannel.de/special/977/index.html)
Kryptographie-Grundlagen (http://www.tecchannel.de/internet/416/index.html)
So funktionieren TCP/IP und IPv6 (http://www.tecchannel.de/internet/209/index.html)
Sicherer Datenaustausch über OpenSSH (http://www.tecchannel.de/software/1117/index.html)

Security im Überblick (Teil 6)

› Im sechsten und letzten Teil unserer Security-Reihe beleuchten wir die Vorzüge und Nachteile verschiedener Architekturen und Protokolle für Virtuelle Private Netze. (VPN).

› VON AXEL SIKORA

Ein Virtuelles Privates Netz (VPN) stellt unter Nutzung einer öffentlichen und unsicheren Infrastruktur die gleichen Merkmale bezüglich Sicherheit, Verwaltung und Durchsatz bereit wie ein Netz, das auf einer privaten Infrastruktur basiert.

Damit ermöglichen VPNs die sichere Kommunikation über unsichere Netze wie speziell das Internet. Sie erlauben damit die kostengünstige, leistungsfähige flexible und sichere Anbindung von Firmenniederlassungen, von Mitarbeitern im Außendienst und Heimarbeitern oder Geschäftspartnern. VPNs bieten also eine Alternative zu Stand- oder Einwahlleitungen über Telekommunikationsnetze, wie sie in herkömmlichen Anbindungen Verwendung finden.

Dabei bezieht sich der Begriff VPN nicht auf eine spezielle Implementierung oder Architektur, sondern stellt eine (oft eher Marketing-getriebene) Bezeichnung für eine Netzankopplung dar, die den Aufgaben der Verschlüsselung und der Authentifizierung besonderes Augenmerk widmet.

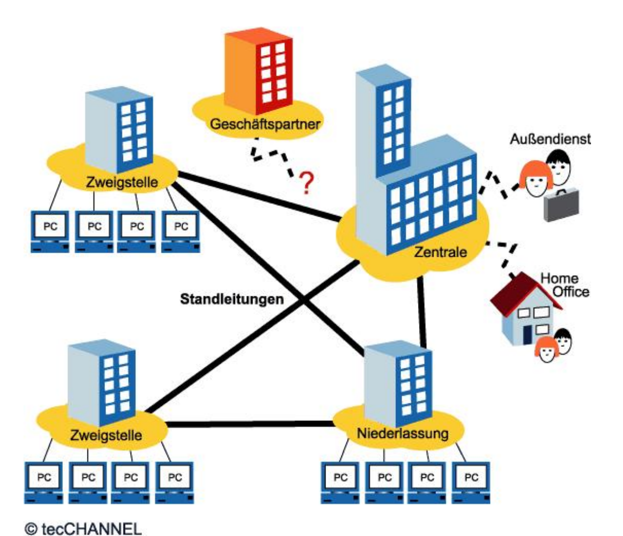
Grundlagen: Security

Die wichtigsten Aspekte zum Thema Sicherheit finden Sie auf über 230 Seiten in unserem tecCHANNEL-Compact "IT-Security", das Sie online (http://www4.websale.net/tecchannel/compact5/) zum Vorzugspreis von 8,90 Euro bestellen oder für 4,90 Euro als PDF downloaden können. In unserem Premium-Bereich (http://www.tecchannel.de/tour3/tour010.html) gibt es diese und weitere tecCHANNEL-Compact-Ausgaben kostenlos zum Download.

› Herkömmliche Netzkopplung

Im herkömmlichen Aufbau von Unternehmensnetzen findet die Kopplung im Wesentlichen in drei Varianten statt:

- › Wählleitungen (Dial-up Lines) greifen unmittelbar auf die Ressourcen der sprachorientierten und leitungsvermittelnden Tk-Netze zurück. Sie kommen überall da zum Einsatz, wo sich Standorte relativ oft verändern oder das Verkehrsaufkommen keine aufwendigere Lösung gestattet.
- › Standleitungen (Leased Lines) stellen im Wesentlichen eine dauernd geschaltete Wählverbindung dar, die zu einem vergleichsweise günstigen Preis angeboten wird.
- › Datenleitungen nutzen paketvermittelnde Netze wie Frame Relay oder ATM.



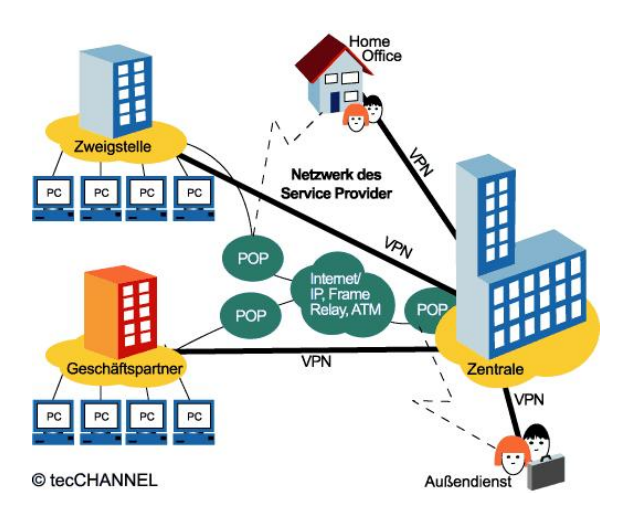
Außen vor: Home Offices, Außendienstmitarbeiter und Geschäftspartner lassen sich nur mit hohem Aufwand in herkömmliche Netzstrukturen integrieren.

Folgende Eigenschaften sind diesen Lösungen (in unterschiedlicher Intensität) gemeinsam:

- › Es fallen relativ hohe Nutzungsentgelte an. Dies gilt insbesondere bei der Überbrückung großer Entfernungen oder bei einer hohen Anzahl zu koppelnder Netzwerke.
- › Es handelt sich - mit Ausnahme der Wählverbindung - um relativ starre Lösungen. Die Dienste werden in der Regel von einem Carrier bereitgestellt und müssen oft manuell eingerichtet werden.
- › Aus dem Transport über die Netze privater Carrier resultiert ein in der Regel sehr hohes Sicherheitsniveau.
- › Bei Verwendung leitungsvermittelnder Netze kann eine unter allen Umständen zur Verfügung stehende Übertragungsbandbreite garantiert werden.

› Kopplung via VPN

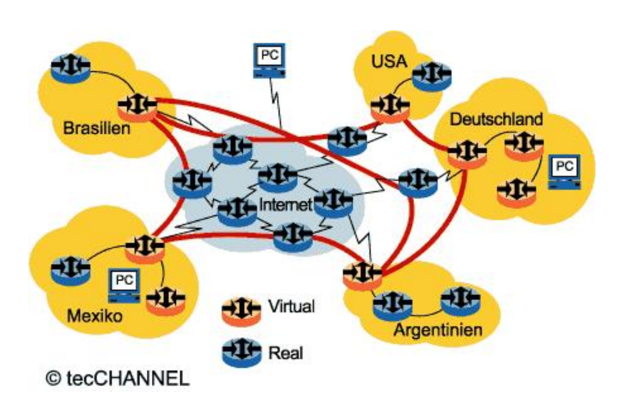
Bei der Kopplung von Unternehmensnetzen über ein VPN nutzt man die Übertragungsressourcen des Internet. Hierzu zählen sowohl die Kapazitäten auf dem Backbone, als auch die weltweit zur Verfügung stehenden Einwahlpunkte.



Zugang für alle: VPNs nutzen die Einwahlknoten und Kapazitäten des öffentlichen Netzwerks.

Daraus resultieren folgende Charakteristika:

- Es fallen gegenüber der herkömmlichen Netzkopplung deutlich geringere Kosten an.
- Verbindungen lassen sich wesentlich flexibler nutzen, da eine bereits bestehende Infrastruktur bedarfsorientiert herangezogen werden kann.
- Die Nutzung des Internet stellt zusätzliche Sicherheitsanforderungen sowohl an die Netzwerk- als auch an die Endknoten.
- Es stehen in aller Regel keine garantierten Bandbreiten zur Verfügung.

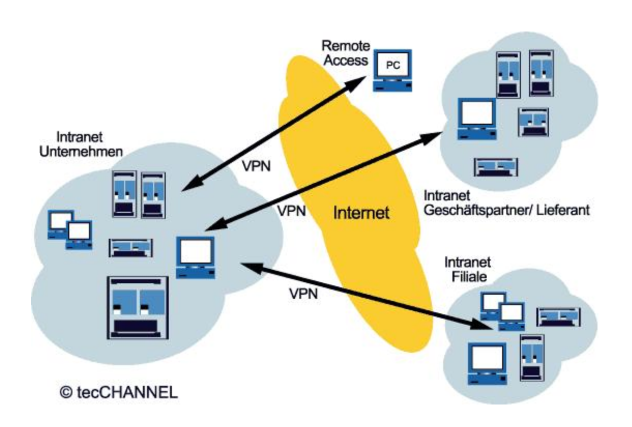


Funktionsprinzip: VPNs bilden logische Netzwerkstrukturen auf eine öffentliche physikalische Topologie ab.

Innerhalb dieser Rahmenbedingungen bildet das VPN eine logische Netzwerkstruktur auf die physische Topologie ab.

› VPN-Architektur

Um eine sichere Übertragung zu erreichen, sind insbesondere Aufgaben der Verschlüsselung und der Authentifizierung zu lösen. Dazu stehen grundsätzlich die in den Teilen 2 bis 5 dieser Reihe vorgestellten Technologien zur Verfügung, die in verschiedenen Architekturen eingesetzt werden können.



Flexibel: VPNs erlauben die Anbindung unterschiedlichster Benutzergruppen an das Unternehmensnetz.

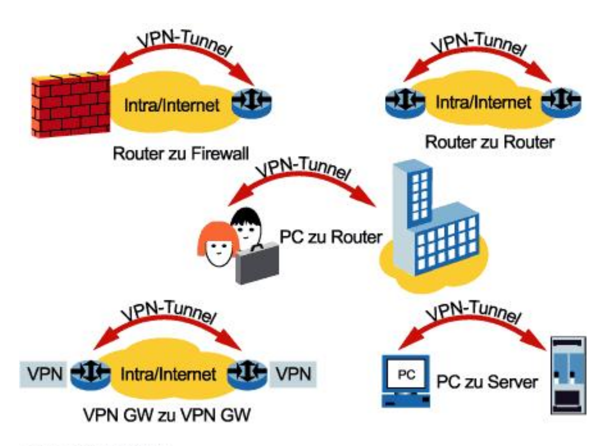
Dabei unterscheidet man bei VPNs generell drei Architekturvarianten:

- Ein Remote-Access-VPN stellt die sichere Verbindung von Home- und Mobile-Workern mit einer Firmenzentrale her. Es ersetzt also die klassische Dial-in-Anbindung über analoge oder ISDN-Wählleitungen. Dabei steigert das VPN die Verfügbarkeit des Zugangs, während sich die Einwahlkosten in der Regel reduzieren.
- Ein Site-to-Site-VPN verbindet verteilte Firmenstandorte über das Internet. Es übernimmt dabei die Rolle, die im klassischen Aufbau Standleitungen beziehungsweise Frame-Relay- oder ATM-Kanäle spielen. Dabei steigt meist die verfügbare Bandbreite, während die Kosten wiederum sinken.

- Ein Extranet-VPN bindet externe Geschäftspartner an. Das vereinfacht und verbilligt die Nutzung von Diensten wie Fax, Mail oder EDI (Electronic Data Interchange).

› Endpunkte

Daneben lassen sich VPNs auch nach der Art der Endpunkte für die sichere Übertragung klassifizieren.



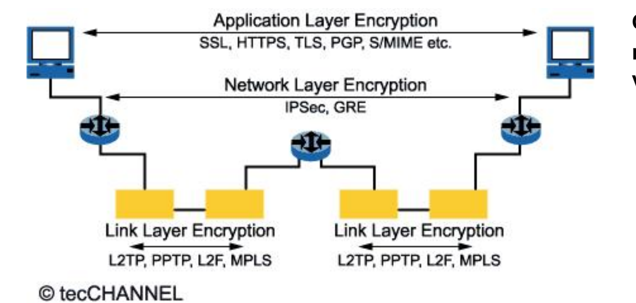
Frage des Endpunkts: Je nach Art der verbundenen Knoten unterscheidet man fünf verschiedene VPN-Varianten.

Hier unterscheidet man im Wesentlichen zwischen den fünf Varianten:

- Router zu Router,
- Router zu Firewall,
- PC zu Router,
- PC zu Server,
- VPN-Gateway zu VPN-Gateway.

› Protokolle

Zur Realisierung eines VPN steht eine Vielzahl von Protokollen zur Verfügung. In der Tat finden sämtliche in den vorangegangenen Teilen dieser Serie erläuterten Protokolle Anwendung.



Qual der Wahl: Zur Implementation von VPNs steht mittlerweile eine Vielzahl von Protokollen zur Verfügung.

Hierbei gilt es insbesondere zu beachten, dass zwar in vielen Fällen die zu Grunde liegenden Verschlüsselungsalgorithmen identisch sind, Architektur und Implementierung sich jedoch unter Umständen in wesentlichen Punkten unterscheiden.

› Wahl der Transportschicht

Eine wesentliche Entscheidung bei der Auswahl einer passenden VPN-Architektur betrifft die Wahl der Schicht, auf der das VPN arbeiten soll. Dabei gilt grundsätzlich: Je tiefer die Schicht angesiedelt ist,

- › desto stärker hängt die Realisierung von den physischen oder logischen Übertragungsmechanismen ab, aber
- › desto weniger hängt sie von den höheren Schichten ab und
- › desto größer fällt meist der zusätzliche Verpackungsaufwand für Tunnelprotokolle aus, da diese in der Regel in den oberen Schichten aufsetzen.

Das wollen wir uns im Folgenden an einigen Beispielen näher ansehen.

› Niedrigere Schichten sind flexibler

Über ein Layer-2-Protokoll wie L2TP lassen sich beliebige Netzwerkprotokolle übertragen, also beispielsweise sowohl IP als auch IPX. Bei Protokollen oberhalb der zweiten Schicht funktioniert das nicht mehr. IPsec etwa ist nur für die sichere Übertragung von IP-Datenverkehr ausgelegt.

Link-Layer-Protokolle erlauben aber auch den transparenten Verkehr des RADIUS-Protokolls. Dass dies nicht immer Vorteile bringt, zeigt beispielsweise der Einsatzbereich von ECP (http://www.tecchannel.de/software/1144/6.html) (PPP Encryption Control Protocol), das in erster Linie bei der Absicherung von Modemzugängen Anwendung findet.

Als Vertreter der Datensicherungsschicht ist ECP allerdings kein Ersatz für Protokolle auf Netzwerk- oder Transportebene. Nur diese gewähren eine durchgehende, anwendungsbezogene Absicherung der Daten.

Die Flexibilität bei Verwendung eines VPN auf einer niedrigeren Schicht muss unter Umständen mit einem deutlich erhöhten Tunnelaufwand erkauft werden. Dies sei am Beispiel des PPTP-Protokolls erläutert, das oberhalb der TCP-Schicht aufsetzt (http://www.tecchannel.de/software/1144/8.html) . Hier müssen die jeweiligen Header mehrfach angehängt werden: TCP-IP-PPTP-TCP-IP-PPP. Das führt zu einem erhöhten Verkehrsaufkommen und zu einem vergrößerten Verarbeitungsaufwand in den VPN-Knoten.

› Höhere Schichten sind sicherer

Ein VPN-Protokoll auf Anwendungsebene wie SHTTP (http://www.tecchannel.de/software/1194/5.html) oder S/MIME ist nur für einen Dienst implementiert. Diese vermeintliche Schwäche lässt sich aber durchaus als zusätzliche Sicherheit für ein Netzwerk auffassen. VPN-Protokolle der niedrigeren Schichten können alle Dienste übertragen. Davon kann man sie zwar durch zusätzliche Filtermechanismen (Paketfilter) abhalten, diese Filterung ist aber inhärent unsicherer als die generelle Nichtverfügbarkeit von Diensten.

Auch SSL kommt stets anwendungsspezifisch zum Einsatz. Ein Anwender, der sich über SSL von außen ins Unternehmensnetzwerk einwählt, kann nur eine einzelne Server-seitige Applikation nutzen. Ein Wechsel der Anwendung während derselben SSL-Sitzung ist nicht möglich. VPN-Verbindungen über IPsec sind dagegen anwendungsunabhängig, der Datenaustausch erfolgt auf der Netzwerkschicht. Es lassen sich entweder zwei Netzwerke oder ein Client mit einem Netzwerk verbinden. Für die Verbindung von Niederlassungen oder mobilen Mitarbeitern mit der Unternehmenszentrale eignet sich auf jeden Fall ein IPsec-VPN besser als eine SSL-Verbindung.

Soll dagegen einer unbekannten Gegenstelle die Nutzung einer Anwendung ermöglicht werden, bietet SSL-Verschlüsselung eindeutig die geeignetere Methode. SSL-Verbindungen können von jedem Terminal aus aufgebaut werden, ohne dass sich die Kommunikationspartner kennen müssen. So lassen sich sensible Daten wie Kreditkartennummer und Bankverbindungen gegen externen Zugriff gesichert über das Internet verschicken.

› L2TP vs. PPTP

Gegenüber dem älteren PPTP (das durch seine Verfügbarkeit auf vielen Windows-Systemen recht große Verbreitung genießt) bietet L2TP eine Reihe von Vorteilen. So kann L2TP beliebige Netzwerkprotokolle in den PPP-Rahmen transportieren. PPTP dagegen befördert nur IP, IPX und NetBEUI. Dies stellt in der Praxis allerdings keine wesentliche Einschränkung dar.

Der Aufbau des Tunnels lässt sich bei PPTP nicht wie bei L2TP an den ISP delegieren. Der mobile PPTP-Client kontaktiert nach erfolgreicher PPP-Verbindung zum ISP eigenständig den PPTP-Server am Übergang zum Firmennetz. Möchte man sich als Administrator der Zeit raubenden Konfiguration von Zieladressen zum PPTP-Server auf den mobilen Clients entledigen, ist L2TP die bessere Wahl.

Gleiches gilt für den Fall, dass mehrere Tunnel zwischen den beiden Kommunikationspartnern betrieben werden sollen. PPTP kann nur einen Hin- und Rückkanal aufbauen, wohingegen das Feld Tunnel ID im Header einer L2TP-Nachricht den Aufbau mehrerer Tunnel ermöglicht.

Darüber hinaus waren bei PPTP Sicherheitslücken in der Microsoft-Implementierung zu konstatieren, die erst nachträglich durch Patches geschlossen wurden. Die Integration von L2TP in Windows 2000 und XP zeigt einen entsprechenden Richtungswechsel auch bei Microsoft an.

› Positionierung von IPsec

IPsec spielt bei der VPN-Realisierung als allgemeine Plattform auf Netzwerkebene für die sichere Übertragung von IP-Datenverkehr eine zentrale Rolle. Deswegen wollen wir hier noch einmal die spezifischen Vor- und Nachteile zusammenstellen.

Zu den Vorteilen zählt, dass:

- IPsec sich für alle Protokolle einsetzen lässt, die via IP übertragen werden können, und
- IPsec die gesamte Kommunikation zwischen zwei Hosts abwickeln kann, wobei ISAKMP die schnelle Etablierung weiterer Security Associations ermöglicht.

Dem stehen jedoch auch gravierende Nachteile gegenüber:

- Der Standard weist eine hohe Komplexität auf.
- Die TCP/IP-Protokollsuite wird modifiziert, was unter Umständen sogar Eingriffe in das Betriebssystem notwendig macht.
- Eine Unterstützung von NAT (Network Address Translation) ist nicht unmittelbar möglich, da der IP-Header mit seinen vermeintlich konstanten Feldern (Quell- und Zieladresse) geschützt wird.

› Risiken von VPNs

Beim Einsatz von VPN sind eine Reihe von Risiken und Nebenwirkungen zu beachten. Einige davon sind technischer Natur, andere betreffen eher das Verhalten der Benutzer.

Hinsichtlich der Technik gilt es, folgende Aspekte zu beachten:

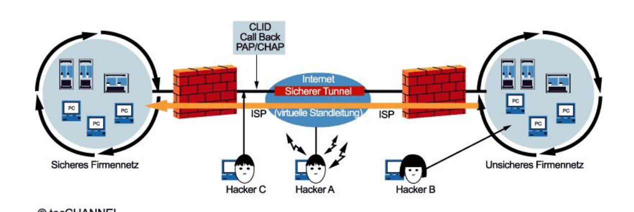
- Nicht alle VPN-Systeme sind sicher gegen Man-in-the-Middle-Angriffe. Dies gilt insbesondere für die Phase des Aushandelns der Übertragungs- und Verschlüsselungsparameter.
- Die Implementierung von VPNs erfordert auf Grund der Vielzahl und Komplexität der verfügbaren Protokolle eine Menge Vorarbeiten. Noch immer treten Inkompatibilitäten zwischen einzelnen Realisierungen auf, so dass momentan eher eine herstellereinheitliche Realisierung zu empfehlen ist.

› Die Realisierung von VPNs erfordert je nach Architektur erhebliche zusätzliche Ressourcen. Dies betrifft nicht nur zusätzliches Equipment, sondern je nach Wahl der Verschlüsselungsverfahren auch einen erhöhten Bedarf an Rechenleistung insbesondere auf den Servern.

› Risikofaktor Mensch

Doch nicht nur die Technik kann die Sicherheit von VPNs einschränken. Auch menschliches Verhalten tritt als zusätzlicher Risikofaktor auf.

So kann einerseits der Einsatz vermeintlich sicherer VPNs dazu führen, dass sich die Benutzer in falscher Sicherheit wiegen und auch sensitive Informationen übertragen, die sie sonst lediglich sicheren Netzen anvertrauen würden.



Bedrohungswechsel: Die schwierig zu knackenden VPNs rücken das Firmennetz als Angriffsziel wieder in den Mittelpunkt.

Andererseits konzentriert sich die Aufmerksamkeit potenzieller Angreifer nach der Implementierung eines VPN wieder verstärkt auf die Firmennetze selbst, da der Übertragungskanal hohe oder unmögliche Hürden stellt.

› Fazit

Trotz zusätzlicher Aufwendungen rechnet sich der Einsatz eines VPN in der Regel bereits nach kurzer Zeit. Dies liegt vor allem an den Vorteilen, die aus den geringeren Leitungsgebühren erwachsen. Hinzu kommt die gestiegene Flexibilität in Bezug auf Anwendungen, Bandbreite und Verfügbarkeit.

Ungeachtet des schon erreichten Komplexitäts- und Sicherheitsniveaus fällt die Voraussage nicht schwer, dass im Bereich der Sicherheitsprotokolle auch künftig viele gleichermaßen interessante wie zunehmend schwer durchschaubare Entwicklungen zu beobachten sein werden. Dafür werden nicht zuletzt die stetig steigenden Fähigkeiten der Angreifer sorgen. (jlu)

Grundlagen: Security

Die wichtigsten Aspekte zum Thema Sicherheit finden Sie auf über 230 Seiten in unserem tecCHANNEL-Compact "IT-Security", das Sie online (http://www4.websale.net/tecchannel/compact5/) zum Vorzugspreis von 8,90 Euro bestellen oder für 4,90 Euro als PDF downloaden können. In unserem Premium-Bereich (http://www.tecchannel.de/tour3/tour010.html) gibt es diese und weitere tecCHANNEL-Compact-Ausgaben kostenlos zum Download.

› Weitere Themen zu diesem Artikel:

Security im Überblick (Teil 1) (http://www.tecchannel.de/software/1068/index.)
Security im Überblick (Teil 2) (http://www.tecchannel.de/software/1095/index.html)
Security im Überblick (Teil 3) (http://www.tecchannel.de/software/1144/index.html)
Security im Überblick (Teil 4) (http://www.tecchannel.de/software/1168/index.html)
Security im Überblick (Teil 5) (http://www.tecchannel.de/software/1194/index.html)
Internet-Router im Eigenbau (http://www.tecchannel.de/betriebssysteme/1200/index.html)
Public-Key-Infrastrukturen (http://www.tecchannel.de/software/1113/index.html)
Workshop: VPN mit Linux (http://www.tecchannel.de/betriebssysteme/897/index.html)
VPN in der Praxis (http://www.tecchannel.de/internet/412/)
VPN: Daten sicher übers Internet (http://www.tecchannel.de/internet/306/index.html)
Drahtlos und sicher
(http://www.tecchannel.de/netzwerk/networkworld/carrier_serviceprovider/208/index.html)
Firewall und VPN in einer Box (http://www.tecchannel.de/netzwerk/networkworld/testcenter/268/)
Sicher durch den Tunnel
(http://www.tecchannel.de/netzwerk/networkworld/technologyupdate/23/index.html)

Kryptographie-Grundlagen

› Die Kryptographie hat längst die Grauzone des Spionagebereichs überschritten und soll für sichere Transaktionen im Internet sorgen. Als Grundlage dienen verschiedenste Verschlüsselungsverfahren.

› VON KLAUS MANHART und ULRICH PROELLER

Verschlüsselungsverfahren kommt im Rahmen der Datenübertragung eine besondere Bedeutung zu. Die Kryptographie soll die Geheimhaltung von Daten ermöglichen. Schließlich hat jede Person und jede Organisation ein legitimes Interesse an dem Schutz seiner Daten vor Ausspähung, sei es im Bereich von vertraulichen Bank- und Börsengeschäften oder sei es die E-Mail mit der Einladung zu einem Bewerbungsgespräch, die der bisherige Arbeitgeber nicht zu Gesicht bekommen soll. Insbesondere Firmen sind darauf angewiesen, ihre Einkaufskonditionen oder ihre Forschungsergebnisse vor den Augen der Konkurrenz zu schützen.

Neben dem offensichtlichen Zweck der Geheimhaltung muss die Kryptographie andere, grundlegende Kriterien erfüllen. Die Authentifizierung, die Integrität und die Verbindlichkeit beim Austausch von empfindlichen Daten sind vor allem für Geschäftsabschlüsse im Internet zwingend erforderlich.

› (Un-)Sicherheitsfaktoren

Die Authentifizierung spielt bei Internettransaktionen eine gewichtige Rolle: Erst der sichere Beweis, dass eine Person auch wirklich die ist, die sie zu sein vorgibt, führt Kunde und Verkäufer zu befriedigenden Geschäftsabschlüssen. Ein kritisches Gebiet findet sich außerdem im Bankgewerbe: Bank und Kunde müssen darauf vertrauen können, dass nur der Kontoinhaber Auskunft über seinen Kontostand bekommt und sich kein Unbefugter unter falschem Namen anmelden kann.

Ein weiterer Unsicherheitsfaktor ist die Integrität der ausgetauschten Daten: Bei abgeschlossenen Transaktionen muss der Empfänger einer Nachricht davon ausgehen können, dass die Nachricht auf dem Weg zu ihm nicht manipuliert wurde. Es wäre fatal, wenn sich bei einer elektronischen Überweisung der Empfänger des Geldes nachträglich verändern ließe.

Erst die Verbindlichkeit sichert einen gelungenen Geschäftsabschluss. Der Absender einer Nachricht darf später nicht leugnen können, dass die Nachricht, zum Beispiel eine Bestellung, tatsächlich von ihm stammt. Damit das Internet als Umschlagplatz für Waren und Dienstleistungen in großem Umfang genutzt werden kann, braucht es deshalb die verbindliche, elektronische Unterschrift (http://www.tecchannel.de/internet/402/index.html) . Sie wird in Zukunft der wohl wichtigste Anwendungsfall für starke Kryptographie sein.

› Starke Kryptographie

Vorneweg gilt es, ein mögliches Missverständnis zu klären. Kryptographie, wie sie hier verstanden wird, hat nichts mit dem Verstecken von Daten ("Security by obscurity") zu tun, wie es zum Beispiel im Bereich der Steganographie (http://www.tecchannel.de/multimedia/377/index.html) angewandt wird.

Die berechnungssichere, so genannte *starke Kryptographie* zeichnet sich im Wesentlichen dadurch aus, dass ihre Algorithmen publiziert und allgemein bekannt sind. Die Entschlüsselung der verschlüsselten Nachricht ist dabei in vertretbarer Zeit ohne Kenntnis des Schlüssels nicht möglich. Die Publikation der Ver- und Entschlüsselungsalgorithmen ermöglicht es den Kryptoanalytikern in aller Welt, das Verfahren auf Herz und Nieren zu überprüfen. Nur ein Algorithmus, der seit einigen Jahren publiziert ist und untersucht wurde, kann als sicher gelten, sofern keine

Schwachstellen gefunden wurden.

Grundsätzlich sind alle gängigen Kryptoalgorithmen durch Ausprobieren zu überwinden. Ob ein Kryptoalgorithmus sicher ist, hängt in der Praxis davon ab, ob der zum Knacken des Algorithmus notwendige Aufwand in Relation gesehen höher ist als der Wert der verschlüsselten Nachricht. Wenn das Ausprobieren selbst mit den schnellsten Computer weitaus länger dauert als die zu lesende Nachricht bedeutsam ist, kann von einem sicheren Algorithmus gesprochen werden. So ist zum Beispiel die Geheimhaltung der Konstruktionspläne eines neuen Autos spätestens nach dessen Markteinführung bedeutungslos. Ein Kryptoalgorithmus, bei dem das Entschlüsseln durch Ausprobieren mehr als zehn Jahre dauert, wäre in diesem Falle also sicher.

› Informationstheorie

Die hohe Redundanz menschlicher Sprache ist eine wichtige Voraussetzung für problemlose Verständigung, weshalb wir unseren Gesprächspartner auch verstehen, wenn es um uns herum sehr laut ist und die Hälfte des Satzes im Lärm untergeht. Wird eine Nachricht per Computer übertragen, ist diese hohe Redundanz unnötig.

Den Unterschied macht folgendes Beispiel deutlich, das den Informationsgehalt eines Satzes hinterfragt. Der Satz: "Ich lese gerade diesen tecChannel-Artikel" besteht (einschließlich Leerzeichen) aus 41 Buchstaben. In der üblichen ASCII-Kodierung würde er 41 Byte, das entspricht 328 Bit, belegen. Tatsächlich beträgt der Informationsgehalt eines Buchstabens gewöhnlicher Sprache statt 8 Bit aber nur 1,0 bis 1,5 Bit, da nicht alle Buchstaben des ASCII-Zeichensatzes vorkommen beziehungsweise gleich häufig sind. Der Informationsgehalt dieses Satzes liegt somit bei etwa 60 Bit. Der Rest, zirka 270 Bit, ist Redundanz, also überflüssige Information.

Die Redundanz macht die zu übertragende Datenmenge nicht nur größer als sie sein müsste. Sie bietet vor allem Kryptoanalytikern einen hervorragenden Ansatz für das Brechen der Verschlüsselung. Denn in jeder Sprache kommen verschiedene Buchstaben unterschiedlich häufig vor. Vor allem bei langen Chiffretexten ist es daher oft möglich, durch ausgefeilte statistische Analysen die Verschlüsselung zu knacken. Um dies unmöglich zu machen, komprimieren moderne Verschlüsselungsverfahren den Text, bevor sie ihn chiffrieren. Die Kompression entfernt einen großen Teil der Redundanz des Textes und macht so *statistische Kryptoanalyseverfahren* weitgehend sinnlos.

› Knackpunkt Rechenpower

Kryptoalgorithmen, bei denen der Aufwand zum Knacken der Verschlüsselung exponenziell mit der Schlüssellänge ansteigt, bieten einen ausreichenden Schutz vor dem wissenschaftlichen und technischen Fortschritt. Denn dieser ist, so paradox dies auf den ersten Blick klingen mag, der größte Feind der Kryptographie. Alle Aussagen über die Sicherheit von kryptographischen Verfahren beruhen auf Abschätzungen zum Rechenaufwand, der erforderlich ist, die Verschlüsselung zu brechen.

Diese Abschätzungen basieren auf der Geschwindigkeit heutiger Rechner und den bekannten mathematischen Verfahren. Die Entwicklung der Verarbeitungsgeschwindigkeit neuer Prozessoren und Rechner lässt sich noch halbwegs vorhersagen. Hier ist mit einer Verzehnfachung der Rechenleistung alle fünf Jahre zu rechnen. Dies gilt aber nur für die heute bekannten, siliziumbasierten Computer. Optische oder biologische Rechner der Zukunft ermöglichen durch massive Parallelverarbeitung eventuell um Zehnerpotenzen höhere Rechengeschwindigkeiten.

Ein ebenso großer Unsicherheitsfaktor ist die künftige Entwicklung der Mathematik. So glaubte man lange Zeit, dass das quadratische Sieb (QS) asymptotisch genauso schnell ist wie jede andere Faktorisierungsmethode. Mit NFS (Number Filed Sieve) wurde eine Faktorisierungsmethode entdeckt, die potenziell bis zu zehn Mal schneller ist als das quadratische Sieb.

› Schlüssellängen

Die Frage nach der richtigen Schlüssellänge lässt sich nicht allgemein beantworten. Es kommt darauf an, wie wertvoll die Daten sind und wie lange sie geheim bleiben müssen.

Eine Sensationsmeldung im Journalismus steht am nächsten Tag in der Zeitung, sie muss also nur bis zur Auslieferung der Zeitung geschützt werden. Dagegen soll die Identität eines Spions auch nach 50 Jahren geheim bleiben. Eine kleine Zusammenstellung minimaler symmetrischer Schlüssellängen findet sich bei Schneier (http://192.168.10.229/internet/416/18.html) :

Empfohlene Schlüssellängen

Informationsart	Lebensdauer	Minimale symmetrische Schlüssellänge
Militärtaktische Informationen	Minuten/Stunden	56-64 Bit
Produktankündigungen, Firmenzusammenschlüsse, Zinssätze	Tage/Wochen	64 Bit
Langfristige Geschäftsplanungen	Jahre	64 Bit
Wirtschaftsgeheimnisse (z.B. Coca-Cola-Rezept)	Jahrzehnte	112 Bit
Geheime Daten zur Wasserstoffbombe	Über 40 Jahre	128 Bit
Personenbezogene Daten	Über 50 Jahre	128 Bit
Geheimdiplomatie	Über 65 Jahre	Mindestens 128 Bit
Daten der US-Volkszählung	100 Jahre	Mindestens 128 Bit

Die angegebenen Schlüssellängen gelten für Schlüssel zu symmetrischen Verfahren. Die für Public-Key-Verfahren verwendeten Schlüssel müssen deutlich länger sein, um die gleiche Sicherheit zu gewährleisten.

Sicherheitsgewährleistung

Symmetrische Schlüssellänge	Asymmetrische Schlüssellänge
56 Bit	384 Bit
64 Bit	512 Bit
80 Bit	768 Bit
112 Bit	1792 Bit
128 Bit	2304 Bit

Längere Schlüssel erhöhen zwar die für das Ver- beziehungsweise Entschlüsseln benötigte Rechenzeit, doch diese Zeiten sind in der Regel so kurz, dass sie nicht ins Gewicht fallen. Es spricht daher wenig dagegen, lange bis sehr lange Schlüssel zu wählen. Es ist niemals sicher auszuschließen, dass die mathematische Wissenschaft oder die Entwicklung neuer, hochspezialisierter Chips zur Kryptoanalyse vermeintlich sichere Schlüssellängen in Zukunft als zu unsicher erscheinen lassen.

› Kryptoalgorithmen

Es gibt zwei Arten von Kryptoalgorithmen mit Schlüsseln: symmetrische Algorithmen und Algorithmen mit öffentlichen Schlüsseln (Public-Key-Algorithmen).

Bei symmetrischen Algorithmen sind Chiffrierschlüssel und Dechiffrierschlüssel entweder identisch, oder der Dechiffrierschlüssel lässt sich aus dem Chiffrierschlüssel berechnen und umgekehrt. Es gilt:

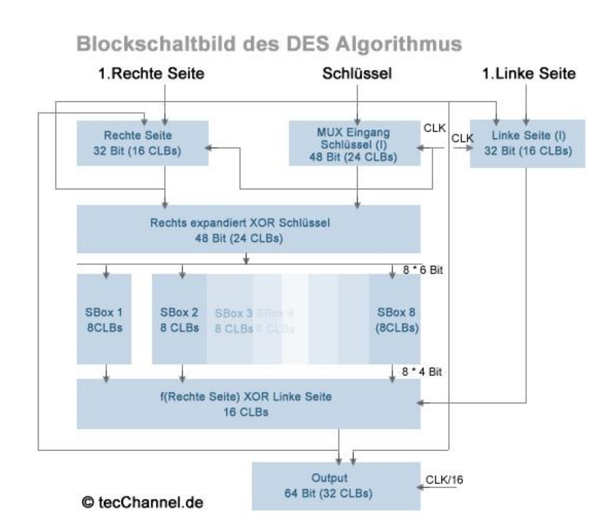
$$E_K(M) = C$$
$$D_K(C) = M$$

M = Klartext Nachricht
C = Chiffretext (verschl. Nachricht)
E = Verschlüsselungsfunktion
D = Entschlüsselungsfunktion
K = Schlüssel

Bei symmetrischen Algorithmen benutzen Sender (oft als Alice bezeichnet) und Empfänger (namentlich Bob) einen gemeinsamen (geheimen) Schlüssel. Dieser geheime Schlüssel muss vor Beginn der verschlüsselten Kommunikation auf eine sichere Weise vereinbart und ausgetauscht worden sein. Zum Beispiel, indem sich Alice und Bob getroffen haben.

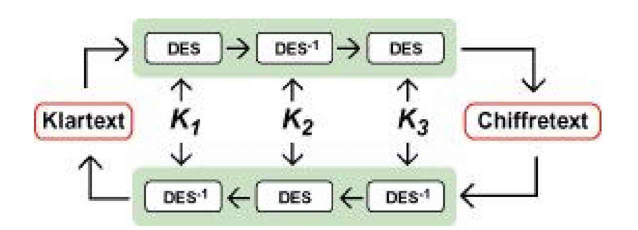
› DES

Das bekannteste und am weitesten verbreitete symmetrische Verschlüsselungsverfahren ist der Data Encryption Standard (DES). Es wurde 1976 in den Vereinigten Staaten als Bundesstandard anerkannt und benutzt eine Schlüssellänge von 56 Bit.



DES: Blockschaltbild des DES-Algorithmus

DES ist auf Standardrechnern in Wochen bis Monaten zu knacken. Anfang 1999 war es möglich, durch die Nutzung der Leerlaufzeit vieler per Internet verbundener Computer, eine per DES verschlüsselte Nachricht innerhalb von 23 Stunden zu dechiffrieren. Erreicht wurde dies einfach durch das Ausprobieren aller möglichen Schlüssel. Spezialrechner brauchen für die gleiche Aufgabe nur einen Bruchteil dieser Zeit. Eine auch heute noch sichere Variante von DES ist Triple-DES, das heißt, die dreimalige, hintereinander geschaltete Anwendung von DES. Die Schlüssellänge steigt dadurch auf 168 Bit.



Dreifach sicher: Beim Triple-DES wird gleich drei Mal verschlüsselt.

Derzeit läuft eine Ausschreibung des NIST für den Advanced Encryption Standard (AES), den Nachfolger von DES. Bei AES soll es sich um einen frei verfügbaren symmetrischen 128-Bit-Blockchiffre handeln. Als Schlüsselgrößen sind 128, 192 und 256 Bit gefordert. In der engeren Auswahl sind seit August 1999 noch fünf Algorithmen, nämlich MARS, RC5, RIJNDAEL, Serpent und Twofish.

› Public-Key-Algorithmen

Algorithmen mit öffentlichem Schlüssel beruhen auf der Tatsache, dass manche Dinge im Leben einfach auszuführen, aber nur schwer rückgängig zu machen sind. Eine Vase aus zehn Metern Höhe fallen zu lassen, bereitet keine große Mühe; aus den Scherben die Vase wieder zusammenzukleben, ist jedoch fast unmöglich.

Bei den Zahlen gibt es ähnliche Phänomene: Zahlen miteinander zu multiplizieren - selbst sehr große - ist leicht. Aber ein Produkt in seine (unbekannten) Faktoren zu zerlegen, ist vergleichsweise schwer.

Bei dem Public-Key-Verfahren wird jeweils vom Sender ein Schlüssel zur Chiffrierung und vom Empfänger ein anderer, zugehöriger Schlüssel für die Dechiffrierung verwendet. Sender und Empfänger verwenden *Schlüsselpaare*. Bei einem guten asymmetrischen Verfahren kann trotz der Kenntnis eines Schlüssels der andere nicht abgeleitet werden. Es gilt:

$$E_{pK}(M) = pC$$
$$D_{sK}(pC) = M$$
$$E_{sK}(M) = sC$$
$$D_{pK}(sC) = M$$

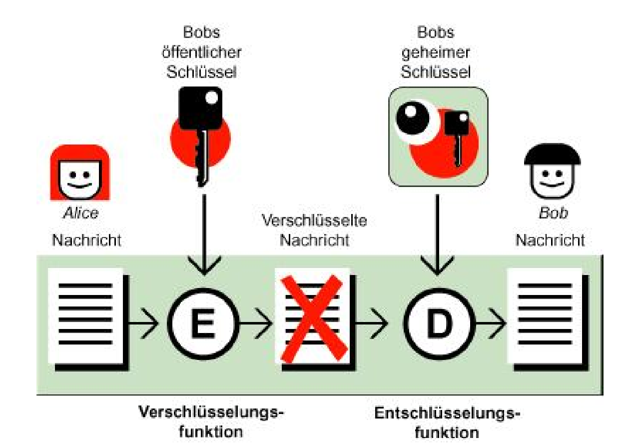
pC = mit öffentlichem Schlüssel verschlüsselte Nachricht
sC = mit privatem Schlüsel verschlüsselte Nachricht
pK = öffentlicher Schlüssel
sK = privater Schlüssel

Zusammengefasst haben Public-Key-Verfahren folgende Merkmale:

- › Jeder potenzielle Kommunikationsteilnehmer besitzt einen öffentlichen Schlüssel (Public Key) und einen persönlichen Schlüssel (Private Key).
- › Der Public Key darf öffentlich bekannt sein, der Private Key muss geheim gehalten werden.
- › Es ist (praktisch) unmöglich, aus dem Public Key den Private Key zu berechnen.
- › Der Sender einer vertraulichen Nachricht muss den Public Key des Empfängers kennen.

› Funktionsweise Public Key

Will Alice eine geheime Nachricht an Bob schicken, verschlüsselt sie die Nachricht mit Bobs öffentlichem Schlüssel. So kann nur Bob diese Nachricht mit seinem privaten Schlüssel (Private Key) wieder entschlüsseln. Es ist dadurch möglich, dass Alice an Bob verschlüsselte Nachrichten schickt, ohne dass die beiden zuvor über einen sicheren Kanal einen gemeinsamen Schlüssel vereinbaren mussten. Das ist der große Vorteil gegenüber den symmetrischen Verfahren.



Getrennt: Beim Verfahren mit Public Keys kommen zwei verschiedene Schlüssel zum Einsatz.

Bei diesem Verfahren spielt es keine Rolle, wer sonst noch Bobs öffentlichen Schlüssel kennt. Eine einmal mit diesem Schlüssel verschlüsselte Nachricht kann nur noch mit Bobs privatem Schlüssel wieder gelesen werden.

› Primfaktorzerlegung

Die Zerlegung einer (großen) Zahl in ihre Primfaktoren ist eines der ältesten Probleme der Zahlentheorie. Neben der versuchsweisen Division, die einfach, aber bei großen Zahlen sehr zeitaufwendig ist, existieren einige effizientere Faktorisierungsalgorithmen, von denen an dieser Stelle nur der neueste und vermutlich bald auch schnellste, das so genannte Zahlenkörpersieb (Number Field Sieve, NFS) genannt werden soll.

Im Moment ist man in der Lage, Zahlen mit etwa 130 Dezimalstellen (entspricht zirka 440 Bit) zu faktorisieren. 1993 benötigte man dazu etwa 5000 MIPS-Jahre (eine theoretische Größe für den Rechenaufwand). Vor einiger Zeit schaltete man über das Internet 1600 Rechner zusammen, die gemeinsam etwa acht Monate brauchten. Nach Aussage der beteiligten Wissenschaftler wäre der Aufwand unter Verwendung des neuen NFS nur ein Zehntel dieser Zeit gewesen. Der Rechenaufwand zur Faktorisierung einer großen Zahl mit n Stellen mit Hilfe des NFS (seine heuristische, asymptotische Laufzeit) lässt sich mit der folgenden Formel abschätzen:

$$e^{(1{,}923+O(1))(\ln(n))^{1/3}(\ln(\ln(n)))^{2/3}}$$

Wie man sieht, steigt der Rechenaufwand mit der Länge der zu faktorisierenden Zahl exponenziell an. Die Primfaktorzerlegung großer Zahlen ist ein seit langem sehr intensiv untersuchtes Problem. Große Fortschritte in Form neuer, wesentlich schnellerer Algorithmen sind daher in diesem Bereich unwahrscheinlich. Dies macht Kryptoalgorithmen, die auf der Primfaktorzerlegung beruhen, zu guten Kandidaten für sichere Kryptoalgorithmen.

› Das BSI empfiehlt

Bei asymmetrischen Verschlüsselungsverfahren haben sich inzwischen eine Reihe unterschiedlicher Methoden etabliert. Vor allem zwei gelten derzeit als sicher und werden unter anderem vom Bundesamt für Sicherheit in der Informationstechnik (BSI (http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/index.htm)) empfohlen:

1. ElGamal, 1985

Das Prinzip des Algorithmus von ElGamal zur asymmetrischen Verschlüsselung beruht auf der Schwierigkeit "diskrete Logarithmen modulo einer Primzahl" zu berechnen. In

praktischen Anwendungen variiert die Primzahl zwischen 512 Bits (geringe Sicherheit) und 1024 Bits (sehr hohe Sicherheit). Eine Variante des ElGamal-Verfahrens ist der 1991 vom National Institute of Standards and Technology publizierte Digital Signature Standard (DSS), der den Digital Signature Algorithm (DAS) spezifiziert. Der ElGamal-Algorithmus ist nicht patentiert.

2. RSA (Rivest, Shamir, Adleman), 1977

RSA, benannt nach den Entwicklern Rivest, Shamir, Adleman, ist das bekannteste Public-Key-Verfahren, die am weitesten verbreitete asymmetrische Verschlüsselungsmethode und ein Quasi-Standard im Internet. Das Prinzip beruht auf der Schwierigkeit, große natürliche Zahlen in der Größenordnung 10 hoch 150 (beispielsweise 200 Dezimalstellen oder 665 Bits) in ihre Primfaktoren zu zerlegen. In praktischen Anwendungen variieren die Zahlen zwischen 512 Bits (geringe Sicherheit) und 2048 Bits (sehr hohe Sicherheit). RSA ist weltweit seit Ende 2000 frei von Patenten.

› RSA

Bei RSA beruhen öffentlicher und privater Schlüssel auf einem Paar sehr großer Primzahlen (100 bis 200 Stellen und mehr). Es wird allgemein angenommen, dass der Aufwand zur Wiederherstellung des Klartextes aus dem Chiffretext und dem öffentlichen Schlüssel äquivalent zur Faktorisierung des Produktes der beiden Primzahlen ist. (Dies ist allerdings streng genommen nur eine qualifizierte Vermutung, es wurde nie bewiesen, dass es wirklich so ist.)

RSA ist um den Faktor 100 bis 1000 langsamer als DES. Dies mag im ersten Moment wie ein Nachteil von RSA aussehen, ist aber tatsächlich eher von Vorteil. Denn für die Ver- und Entschlüsselung von normalen Mitteilungen fällt diese Zeit praktisch nicht ins Gewicht. Wer aber RSA mittels einem Brute-Force-Angriff, also dem Ausprobieren aller möglichen Schlüssel, brechen möchte, tut sich umso schwerer, je langsamer der Algorithmus ist.

Es ist zurzeit möglich, einen 512-Bit-langen RSA-Schlüssel zu knacken. Der Aufwand hierfür beträgt im Moment etwa 8000 MIPS-Jahre. Schlüssellängen von 1024 Bit oder gar 2048 Bit sind bei RSA nach menschlichem Ermessen in nicht absehbarer Zukunft absolut sicher.

› Schlüsselgenerierung bei RSA

1. Schritt: Der Sender, A, wählt zwei große Primzahlen **p** und **q**. A berechnet das Produkt **n = p * q**. Wichtig: p und q müssen sich in ihrer Länge deutlich unterscheiden. Andernfalls könnten sie aus n leicht bestimmt werden, indem in der Umgebung von (Wurzel aus n) alle Primzahlen getestet werden.

2. Schritt: A wählt seinen öffentlichen Schlüssel **e** so, dass e und **(p-1) * (q-1)** keinen gemeinsamen Primfaktor außer der 1 haben.

3. Schritt: A berechnet seinen privaten Schlüssel **d** mit Hilfe der Formel: **ed = 1 mod ((p-1) * (q - 1))**. Das bedeutet: Zur Berechnung seines privaten Schlüssels ist die Kenntnis von p und q erforderlich, die daher ebenfalls geheim gehalten werden müssen.

Die Zahlen e und n bilden den öffentlichen Schlüssel, d ist der private Schlüssel. Die beiden, zur Generierung der Schlüssel verwendeten Primzahlen, können jetzt verworfen werden, denn sie werden nicht mehr benötigt. Selbstverständlich dürfen sie niemals bekannt gegeben werden.

Zur Verschlüsselung einer Nachricht wird diese in Blöcke zerlegt, deren Länge sich aus der größten Zweierpotenz bestimmt, die kleiner ist, als n Stellen hat. Die Verschlüsselung erfolgt mit:

$c_i = m_i^e \bmod n$ **für alle Nachrichtenblöcke** m_i

Die Entschlüsselung der verschlüsselten Blöcke **ci** erfolgt mit

$$m_i = c_i^d \bmod n$$

› Sicherheit von RSA

Wesentlich für die Sicherheit von RSA ist die Auswahl geeigneter Primzahlen. Sie müssen erstens zufällig gewählt werden und zweitens groß genug sein, um bei steigender Rechenleistung auch in zehn oder 20 Jahren noch einer Primfaktorzerlegung standhalten zu können. Sehr leistungsfähige Rechner könnten in den nächsten Jahren die den Einwegfunktionen zu Grunde liegenden Gleichungen umkehren. Man sollte deshalb im Zweifelsfall eine große Schlüssellänge wählen.

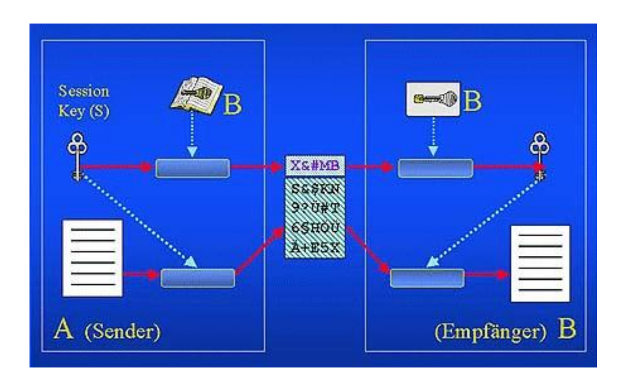
Das BSI verlangt in einem Papier (http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/index.htm) für den Modulus **n = p * q** eine Bitlänge von mindestens 2048. Für den Zeitraum bis Ende 2004 genügen noch 1024 Bit.

Compaq hat aktuell eine effizientere Methode für die RSA-Verschlüsselung entwickelt. Beim MultiPrime-Verfahren basiert der geheime Schlüssel nicht wie üblich auf nur zwei, sondern auf drei oder mehr Primzahlen. Dadurch sollen Entschlüsselung und Signatur deutlich schneller und ressourcensparender durchzuführen sein. Den Modulus auf drei Primzahlen zu verteilen bewirkt nach Compaq-Angaben eine theoretische Geschwindigkeitssteigerung um den Faktor 6,7. RSA Security (http://www.rsasecurity.com) verspricht sich auch in SmartCards zumindest eine Verdopplung der Performance.

Operationen mit den dazu gehörenden öffentlichen Schlüssel (Verschlüsselung und Signaturprüfung) dagegen sind von dem Verfahren nicht betroffen. RSA Security hat MultiPrime in seine Entwicklerkits und Libraries.

› Hybride Verschlüsselung

Da asymmetrische Verschlüsselungssysteme in der Regel sehr viel langsamer arbeiten als symmetrische Algorithmen, werden bei den im Internet gebräuchlichen Verschlüsselungsprogrammen häufig beide Verfahren eingesetzt. Bei einem Verbindungsaufbau wird zunächst mit Hilfe einer asymmetrischen Verschlüsselung ein Sitzungsschlüssel (*Session Key*) gesichert übertragen. Dieser wird anschließend für eine symmetrische Verschlüsselung genutzt. Durch diese Kombination - man spricht von hybrider Verschlüsselung - vereinigt man einen gesicherten, aber langsamen Schlüsseltausch mit einer schnellen, aber weniger sicheren Verschlüsselung.



Das Beste zweier Welten: Hybridverfahren mit asymmetrischer/symmetrischer Verschlüsselung. (Quelle Teletrust)

Das Hybridverfahren läuft wie folgt ab: Der Sender A erzeugt in seiner vertrauenswürdigen Umgebung einen möglichst zufälligen symmetrischen Schlüssel S, den so genannten *Session Key* und kodiert mit diesem seine Nachricht. Diesen Schlüssel selbst chiffriert der Sender mit dem öffentlichen (asymmetrischen) Schlüssel des Empfängers B. Beides, die mit S verschlüsselte Nachricht und der mit dem öffentlichem Schlüssel von B kodierte Sitzungsschlüssel, werden nun an den Empfänger übermittelt.

Da der Empfänger B den Sitzungsschlüssel nicht kennt, muss er zunächst den chiffrierten (symmetrischen) Sitzungsschlüssel entschlüsseln. Dies erfolgt mit seinem geheimen (asymmetrischen) Schlüssel. Den so gewonnenen Sitzungsschlüssel S kann er nun dazu verwenden, die chiffriert übermittelte Nachricht wieder zu dechiffrieren und somit Kenntnis des Nachrichteninhalts zu erlangen.

› Kryptoanalytische und andere Angriffe

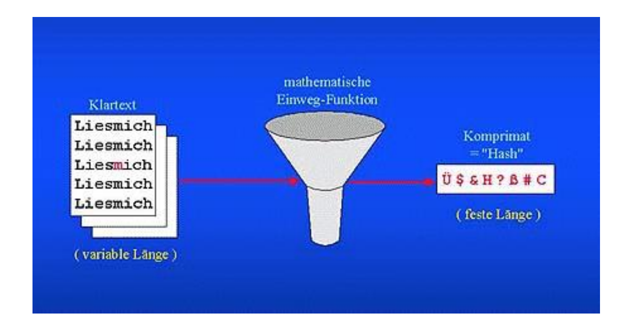
Es gibt verschiedene Möglichkeiten zum Angriff gegen kryptographische Protokolle. Am offensichtlichsten ist der Weg des Brute-Force-Angriffs. Bei ihm werden einfach so lange alle möglichen Schlüssel auf den chiffrierten Text angewandt, bis der lesbare Klartext vorliegt. Daneben gibt es, je nach Algorithmus, mathematisch oft sehr anspruchsvolle Analysemöglichkeiten, die auf bestimmten Eigenheiten des verwendeten Kryptoalgorithmus aufsetzen. Gute Kryptoalgorithmen zeichnen sich dadurch aus, dass der Aufwand für derartige Angriffe genauso groß oder größer als der Aufwand eines Brute-Force-Angriffs ist.

In der Praxis ist jedoch das Risiko, das aus der Ausspähung eines Schlüssels oder dessen Gewinnung durch Bestechung, Erpressung oder Drohung mit Gewalt erwächst, um Größenordnungen höher, als das Risiko, das aus kryptoanalytischen Angriffen resultiert. Die Frage des sicheren Austausches und der absolut sicheren Aufbewahrung von Schlüsseln hat daher eine besondere Bedeutung.

Der sicheren Kommunikation droht noch aus einer anderen Richtung Gefahr. Staatliche Institutionen tun sich noch immer sehr schwer mit der Möglichkeit des Bürgers, unbelauscht zu kommunizieren. Zu sehr haben sich NSA, FBI, die Bundes- und Landeskriminalämter und der Verfassungsschutz daran gewöhnt, jederzeit Zugriff auf alle sie interessierenden Daten der Bürger zu bekommen. Ein Mensch, der Wert darauf legt, seine alltägliche Kommunikation unbelauscht von nationalen und internationalen Organisationen zu praktizieren, gerät leicht in den Verdacht, etwas Verbotenes zu tun. Einschlägige Politiker und Sicherheitsexperten sind dann schnell mit dem Argument zur Hand, wer nichts zu verbergen habe, brauche auch keine Angst vor staatlicher Überwachung zu haben.

› Hash-Funktionen für Signaturen

Verschlüsselungsverfahren wie RSA erreichen nur den Schutz der Vertraulichkeit einer Nachricht. Neben den eigentlichen Signaturverfahren zum Schutz der Vertraulichkeit benötigt man noch eine Methode, den Urheber einer Nachricht beweisbar zu dokumentieren. In der Regel erfolgt dies mit kryptographischen Prüfsummen, so genannten *Hash-Funktionen* . Das sind mathematische Methoden, die aus einem beliebigen Klartext nach einem vorbestimmten Verfahren eine Prüfziffer (Komprimat) generieren. Die Funktion verwandelt einen Klartext so in ein entsprechendes Komprimat um, dass auch die kleinste Veränderung des ursprünglichen Texts zu einer gänzlich anderen Prüfziffer führt.



Nicht umkehrbar: das Ergebnis der Hash-Funktion (Quelle Teletrust)

Es gehört zu den Forderungen an diese mathematische Funktion, dass aus dem einmal erzeugten Komprimat der ursprüngliche Text nicht wieder rekonstruiert werden kann. Eine solche Hash-Funktion ist nicht umkehrbar und gilt somit als Einwegfunktion. Anders als beim Chiffrieren, ist also eine Wiederherstellung des ursprünglichen Textes nicht

möglich.

Außerdem muss die Hash-Funktion möglichst *kollisionsfrei* sein. Verschiedene Nachrichten mit gleichem Hashwert sollen möglichst selten vorkommen. So ist mit einer praktisch vernachlässigbaren Unsicherheit ein bestimmter Hashwert das Ergebnis eines und nur eines ursprünglichen Klartextes.

Der Vorteil dieses Verfahrens liegt in der Tatsache, dass anstatt des gesamten Textes lediglich ein kurzer Hashwert besonders geschützt werden muss.

› Hash-Funktionen in der Praxis

Für digitale Signatur-Verfahren ist die Festlegung auf eine Hash-Funktion notwendig. Verfügbare Einweg-Hash-Funktionen sind:

SHA/SHA-1 (Secure Hash Algorithm One)

SHA wurde von der NSA entwickelt und als US-Standard angenommen. Eine leicht modifizierte Form hat als SHA-1 den Algorithmus inzwischen ersetzt. Der mit SHA-1 erzeugte Hashwert wird für den DSA (Digital Signature Algorithm), der im DSS (Digital Signature Standard) spezifiziert wird, benötigt. Der Hashwert hat eine Länge von 160 Bit.

MD2, MD4, MD5 (Message Digest)

MD4 und MD5 sind Hash-Funktionen, die von R. Rivest (RSA Laboratories) entwickelt und im Zusammenhang mit dem PEM-Standard (Privacy Enhanced Mail) vorgestellt wurden. MD5 ist eine Weiterentwicklung von MD4. Die Algorithmen erzeugen einen Message Digest (Hashwert) von 128 Bit Länge.

RIPEMD-128, RIPEMD-160 (RIPE-Message Digest)

RIPEMD wurde im Rahmen des EU-Projektes RIPE (RACE Integrity Primitives Evaluation, 1988-1992) ins Leben gerufen. (RIPE-Message Digest). Wegen kryptographischer Schwächen von MD4 und MD5 wurde RIPEMD von Hans Dobbertin, Antoon Bosselaers und Bart Preneel entwickelt. Der Hashwert ist entweder 128 Bit (RIPEMD-128) oder 160 Bit (RIPEMD-160) lang.

RSA Data Security hat auf Grund der Schwächen verfügt, dass MD4 und MD5 für zukünftige Hash-Funktionen nicht implementiert werden sollte. Generell bieten Hash-Funktionen mit längeren Prüfziffern höhere Sicherheit. Daher sollten zukünftig SHA-1 oder RIPEMD-160 verwendet werden. RIPEMD-160 scheint sich in Europa und SHA-1 in den USA als de facto Standard durchzusetzen.

Erst die Kombination aus asymmetrischen Verschlüsselungsverfahren und Hashwerten bietet die Möglichkeit, ein Analogon zur menschlichen Unterschrift zu erzeugen.

› Fazit

Der Mittels der Kryptographie unternommene Versuch, Daten über verschiedenste Verschlüsselungsmethoden geheim zu halten, dient der Absicherung des individuellen Rechts auf Unantastbarkeit der Privatsphäre (http://www.tecchannel.de/tecvision/191/index.html) . Denn gerade diese gilt es im Datenrausch des Internets zu schützen, sei es bei Bestellungen (http://www.tecchannel.de/internet/394/index.html) , Bankgeschäften (http://www.tecchannel.de/internet/62/index.html) , beim normalen E-Mail-Verkehr (http://www.tecchannel.de/internet/398/index.html) oder beim generellen Surfen (http://www.tecchannel.de/internet/395/index.html) durch das Internet mittels entsprechender Absicherungsmethoden (http://www.tecchannel.de/internet/284/index.html) .

Wie jeher, zeigen sich zwei Seiten - einerseits der Versuch, Daten zu schützen und damit einhergehend Versuche, diesen Schutz aufzubrechen. Allerdings tragen Aufklärungsversuche in den Medien langsam Früchte.

Wachsende Sensibilisierung der Bürger, mehr aber noch der massive Druck der Industrie, die ein vitales Interesse an sicherer Kommunikation hat, haben im vergangenen

Jahr zu einer deutlichen Liberalisierung auf diesem Gebiet geführt. Das am meisten verbreitete Programm zur sicheren Verschlüsselung von E-Mails, PGP (http://www.pgpi.org/) (Pretty Good Privacy), durfte jahrelang nicht aus Amerika exportiert werden, weil es militärisch(!) sensible Technologie enthielt. Nur über den Umweg, den gedruckten Sourcecode von USA nach Europa zu schaffen, hier wieder einzuscannen und neu zu übersetzen, war es möglich, PGP auch im Rest der Welt zu nutzen. Dieser absurde Zustand ist inzwischen glücklicherweise beseitigt. Trotzdem muss auch weiterhin sorgsam darauf geachtet werden, dass staatliche Behörden sich nicht erneut Hintertürchen schaffen, um die Bevölkerung oder die Wirtschaft zu belauschen. (sda/mha)

Wozu man diese kryptographischen Verfahren benötigt, lesen Sie in einem gesonderten Beitrag zur digitalen Signatur (http://www.tecchannel.de/internet/402/index.html) , die bald auch virtuelle Behördengänge über das Internet ermöglichen soll.

Literatur:

A.K. Lenstra and H.W. Lenstra, Jr., eds., Lecture Notes in Mathematics 1554: The Development of the Number Field Sieve, Springer-Verlag, 1993

C.E. Shannon, Collected Papers: Claude Elmwood Shannon, N.J.A. Sloane and A.D. Wyner, eds., New York: IEEE Press, 1993

Schneier, Bruce (1996): Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C; Addison-Wesley

› Weitere Themen zu diesem Artikel:

- Elektronisch unterschreiben (http://www.tecchannel.de/internet/402/index.html)
- Ist Privatsphäre noch möglich? (http://www.tecchannel.de/tecvision/191/index.html)
- Dem Surfer auf der Spur (http://www.tecchannel.de/internet/284/index.html)
- Sichere E-Mail (http://www.tecchannel.de/internet/398/index.html)
- Safer Surfen (http://www.tecchannel.de/internet/395/index.html)
- Versteckter Schutz gegen Datenraub (http://www.tecchannel.de/multimedia/377/index.html)
- Bezahlen im Internet (http://www.tecchannel.de/internet/394/index.html)
- HBCI - Der neue Homebanking-Standard (http://www.tecchannel.de/internet/62/index.html)

Praxis der digitalen Signatur

› Rechtlich ist die handschriftliche Unterschrift der digitalen Signatur gleichgesetzt. Doch in der Praxis verhindern fehlende Anwendungen und Standards die Ausbreitung der elektronischen Unterschrift.

› VON KLAUS MANHART

Die juristischen Grundlagen für die digitale Signatur sind gelegt. Doch so recht in Schwung kommt sie nicht. Weder Privatanwender noch Unternehmen setzen in nennenswertem Ausmaß auf die elektronische Unterschrift. Die mangelhafte Infrastruktur sowie fehlende Standards hemmen die Ausbreitung der elektronischen Unterschrift ganz entscheidend.

Firmen schrecken dadurch vor größeren Investitionen zurück. Und im Privatbereich fehlen die Anwendungen. Doch die Optimisten unter den Sicherheitsexperten rechnen damit, dass diese Hindernisse in den nächsten Monaten weit gehend verschwinden.

Sicher ist derzeit allein die rechtliche Basis. Seit Mai letzten Jahres ist das neue Signaturgesetz (http://jurcom5.juris.de/bundesrecht/sigg_2001/index.html) in Kraft, das eine EU-Richtlinie umsetzt und das alte, sehr restriktive Gesetz aus dem Jahr 1997 ablöste. Mit Inkrafttreten des Gesetzes können Bürger und Unternehmen Dokumente digital unterschreiben.

› Typen von Signaturen

Die letzten Hürden auf dem Weg zur endgültigen Gleichstellung von handschriftlicher und elektronischer Unterschrift wurden Mitte 2001 beseitigt. Mit dem am 1. August 2001 in Kraft getretenen Gesetz zur Anpassung der Formvorschriften des Privatrechts (http://217.160.60.235/BGBL/bgbl1f/b101035f.pdf) wurden Gesetzesartikel und Vorschriften an die Erfordernisse des Signaturgesetzes angeglichen. Elektronische Unterschriften, die bestimmte Voraussetzungen erfüllen, sind damit den handschriftlichen gleichgestellt. Der online geschlossene Vertrag hat damit den gleichen Stellenwert wie der Papiervertrag.

Im Detail sieht der deutsche Gesetzgeber in dem novellierten Signaturgesetz vier verschiedene Typen von Signaturen vor:

- (Einfache) elektronische Signatur (§ 2 Nr. 1 SigG), (Stufe 1)
- fortgeschrittene elektronische Signatur (§ 2 Nr. 2 SigG), (Stufe 1)
- qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG) und (Stufe 2)
- qualifizierte elektronische Signatur mit Anbieter-Akkreditierung (§ 15 Abs. 1 Satz 4 SigG) (Stufe 3)

› Weiche und qualifizierte Signatur

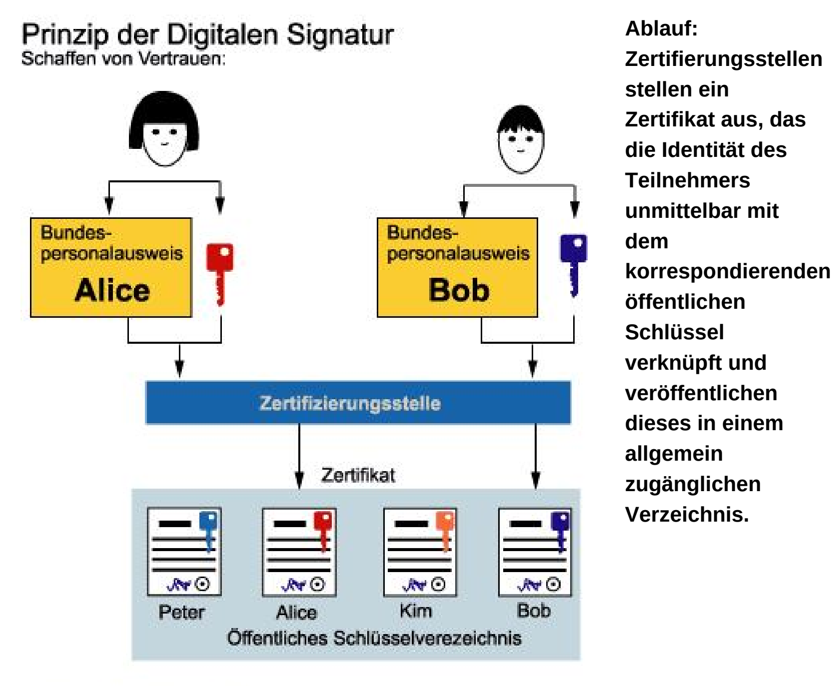
Einfache und fortgeschrittene elektronische Signaturen bilden die "weichen" Signaturen, die nach EU- und deutschem Recht der handschriftlichen Unterschrift nicht gleichgestellt sind. Solche Signaturen kann man zum Beispiel mit dem Freeware-Programm PGP (http://www.pgpi.org) (Pretty Good Privacy) erzeugen. Sie lassen sich für einfache Transaktionen wie dem Verschicken von Mails, dem CD-Kauf im Internet oder innerhalb eines Unternehmens einsetzen und unterliegen der freien Beweiswürdigung der Richter. Beide Signaturen bieten nur wenig Sicherheit und ermöglichen keine eindeutige Zuordnung einer Willenserklärung zu einer Person.

Der handschriftlichen Unterschrift juristisch gleichgestellt ist erst die qualifizierte elektronische Signatur ab Stufe 2. Nur sie hat vor Gericht Beweiskraft und bildet praktisch

den EG-Mindeststandard für Signaturen. Solche Signaturen sind durch Verschlüsselungsverfahren mit dem Dokument, das sie unterzeichnen, verknüpft. Der Empfänger kann hier immer erkennen, ob Dokumente durch Dritte manipuliert worden sind. Wichtig bei dieser Stufe: Qualifizierte Signaturen ab Stufe 2 müssen von einem Zertifizierungsdienst (Trustcenter) anerkannt sein. Die Anforderungen an diese Trustcenter - auch Certification Authorities (CA) - bilden den wesentlichen Teil des Signaturgesetzes.

› Mangelware Trustcenter

CAs liefern mit digitalen Zertifikaten und Schlüsseln die Grundausstattung zur Teilnahme am rechtsverbindlichen und vertraulichen elektronischen Geschäftsverkehr. Sie überprüfen zunächst die Identität des Nutzers und generieren einen elektronischen Ausweis - das Zertifikat.



Ablauf: Zertifizierungsstellen stellen ein Zertifikat aus, das die Identität des Teilnehmers unmittelbar mit dem korrespondierenden öffentlichen Schlüssel verknüpft und veröffentlichen dieses in einem allgemein zugänglichen Verzeichnis.

Dieses beinhaltet den Namen des Ausstellers, Informationen über die Identität des Inhabers, Mail-Adresse sowie die digitale Signatur des Ausstellers. Vor allem aber bestätigt das Zertifikat, dass der öffentliche Schlüssel wirklich der beantragenden Person gehört. Der öffentliche Schlüssel ist ein eindeutiges Merkmal zur Identifizierung.

› Typen von Zertifizierungsdiensten

Nach dem Signaturgesetz gibt es zwei Typen von Zertifizierungsdiensten. Bei einem "angemeldeten Zertifizierungsdienst" reicht eine Erklärung über die Sicherheit aus. Er ist nur bei den zuständigen Behörden gemeldet, aber keinerlei behördlicher Kontrolle unterworfen. Im Falle eines Rechtsstreits muss die Sicherheit vom Zertifikatnehmer - Unternehmen oder Privatanwender - bewiesen werden.

Im Gegensatz dazu überprüfen und bestätigen bei "akkreditierten Zertifizierungsdiensten" unabhängige Dritte die Sicherheit. Zertifikate dieser Stufe dürfen nur Trustcenter vergeben, die von der Regulierungsbehörde für Post und Telekommunikation einen Prüfstempel erhalten haben.

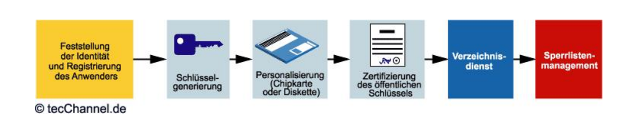
Nur sie dürfen "qualifizierte elektronische Signaturen mit Anbieterakkreditierung" oder vereinfacht: "Signaturen mit gesetzlichem Gütesiegel" ausstellen. Solche Signaturen sind also "besonders sicher". Mit diesem Signatur-Typ ermöglichte es die EU-Richtlinie den

Mitgliedstaaten, im Bereich der Kommunikation mit Behörden hohe Anforderungen zu stellen.

› Praxis der Zertifizierung

Wie läuft der Zertifizierungsprozess praktisch ab? Das Trustcenter erzeugt das Signaturschlüsselpaar - den privaten und den öffentlichen Schlüssel - und lädt sie auf eine Chipkarte. Die Chipkarte wird anschließend an den Antragsteller übergeben, zusammen mit einer zur Chipkarte gehörenden Geheimnummer (PIN).

Soll ein Dokument digital signiert werden, verknüpft der Absender das zu versendende Dokument mit seinem privaten Schlüssel, indem er die Chipkarte in den Chipkartenleser steckt und in der entsprechenden Software den Befehl "Signieren" anklickt. Das auf diese Weise erzeugte Dokument dient als digitale Signatur und wird an das ursprüngliche Dokument angehängt. Beide Teile werden anschließend zusammen übermittelt.

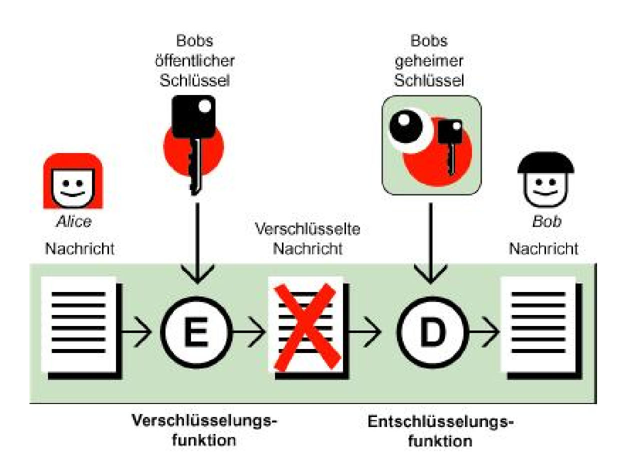


Sechs Stufen: Grundlegender Ablauf des Zertifizierungsprozesses.

Der Empfänger des so signierten Dokuments kann den Inhalt sofort im Klartext lesen. Allerdings besteht noch keine Gewähr für den richtigen Absender und den korrekten Inhalt des Dokuments.

› Öffentlicher Schlüssel für den Empfänger

Um Inhalt und Absender zu prüfen, muss der Empfänger die digitale Signatur mit dem öffentlichen Schlüssel des Absenders entschlüsseln. Dazu muss er im Besitz dieses öffentlichen Schlüssels sein, der beispielsweise künftig in einem Verzeichnis, ähnlich dem Telefonbuch, abgelegt sein kann.



Öffentlicher und geheimer Schlüssel: Das Grundprinzip der Public-Key-Verschlüsselung.

Derzeit gibt es nur wenige Trustcenter, die ihre Arbeit aufgenommen haben. Eines der Haupthindernisse waren bislang die hohen Investitionskosten von über fünf Millionen Euro für Gebäude und Sicherheitsinfrastruktur. Mit dem neuen Signaturgesetz hat sich die Situation verbessert. Zertifizierungsanbieter müssen nun nicht mehr alle Dienstleistungen selbst erbringen, sondern können Teile von anderen Zertifizierungsstellen beziehen.

Die Übertragbarkeit geht so weit, dass sogar die Ausfertigung der Zertifikate und die Produktion der Chipkarten ausgelagert werden darf. Dadurch lassen sich die nötigen Investitionen für den Aufbau der akkreditierten Zertifizierungsstellen deutlich verringern. Beobachter rechnen damit, dass mittelfristig 20 Trustcenter verfügbar sind.

› Zertifikate für Privat- und Geschäftskunden

Aktuell sind allerdings gerade mal ein halbes Dutzend akkreditierte Trustcenter verfügbar, von denen zudem ein Teil nur beschränkte Nutzergruppen wie Notare zertifiziert. Allgemein zugängliche CAs betreiben die Deutsche Post Tochter Signtrust und das TC Trustcenter aus Hamburg. Sie bieten sowohl Privat- als auch Geschäftskunden Zertifikate an.

Diese kosten je nach Anbieter zwischen 25 und 150 Euro im Jahr. Dafür erhält man neben einer Chipkarte mit der Signatur meist auch gleich den passenden Kartenleser mit PC-Anschluss und Programme zur Integration der Chipkarte in die vorhandene Software-Umgebung.

Die anderen bisher akkreditierten Zertifizierungsstellen richten sich vornehmlich an geschlossene Benutzergruppen oder ausschließlich an Geschäftskunden. So sind die Zertifikate der Datev eG nur für Steuerberater verfügbar, während die Telekom-Zertifizierungsstelle TeleSec auf Geschäftskunden zielt. Eine Liste aller aktuell akkreditierten Zertifizierungsdienste hat die Regulierungsbehörde (http://www.regtp.de/tech_reg_tele/in_06-02-02-00-00_m/06/index.html) für Post und Telekommunikation zusammengestellt.

› Signtrust

Von den bisher akkreditierten Zertifizierungsstellen macht Signtrust (http://www.signtrust.de) mit einem Startpaket derzeit das günstigste Angebot. Für 61,36 Euro erhalten Interessenten neben dem elektronischen Signatur-Zertifikat auf einer Chipkarte auch einen Kartenleser mit PC-Anschluss. Im Preis eingeschlossen ist bereits die erste Jahresgebühr, jedes weitere Jahr sind 25,56 Euro fällig.

Um an das Zertifikat zu gelangen, meldet man sich online bei Signtrust an und druckt dann den Antrag aus. Anschließend legt der Antragsteller diesen zusammen mit einer Ausweiskopie und dem Original des Ausweises einer beliebigen Postfiliale vor, wo eine Überprüfung der Identität durchgeführt wird. Aus Sicherheitsgründen erhält der Signtrust-Kunde zwei Lieferungen- die Chipkarte mit der elektronischen Signatur, den Chipkartenleser, das Software-Paket Signtrust Mail sowie eine PIN-Nummer.



Signtrust: Das Signtrust-Mailmenü unter MS-Outlook

Praktisch läuft der Signierprozess wie folgt ab: Der Anwender schreibt seine E-Mail mit Hilfe seines E-Mail-Programms - derzeit werden nur Microsoft Outlook oder Lotus Notes bedient. Signtrust Mail stellt dann in dem Mail-Programm die zusätzlichen Funktionen "Nachricht signieren" und "Nachricht verschlüsseln" zur Verfügung.

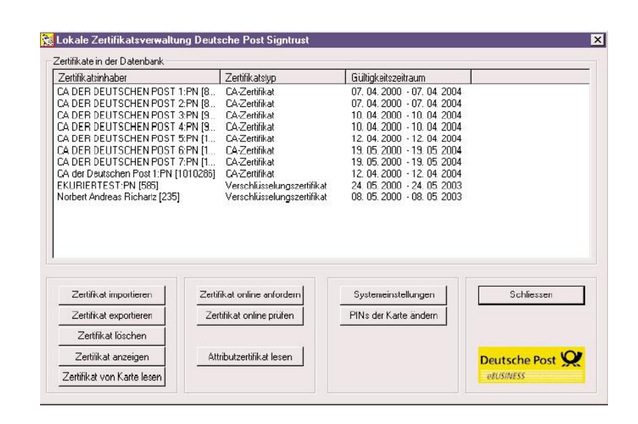
› Signtrust in der Praxis

Nachdem der Anwender seine Signtrust Signaturkarte in den Chipkartenleser eingeführt hat, wählt er durch Anklicken die Funktion "Nachricht signieren" aus. Daraufhin wird ihm seine E-Mail durch Signtrust Mail in einem eigenen Fenster erneut präsentiert.



Signtrust: Das Informationsfenster nach einer erfolgreichen Signaturprüfung

Durch diese zusätzliche Darstellung wird sichergestellt, dass er wirklich nur das unterschreibt, was er auch auf dem Bildschirm gesehen und akzeptiert hat. Wenn er mit seiner E-Mail in der angezeigten Form einverstanden ist, aktiviert er die Signaturfunktion seiner Signaturkarte durch Eingabe seiner PIN.



Signtrust: Die Zertifikatsverwaltung unter Signtrust Mail

Seine Mail wird dann von Signtrust Mail digital signiert und abgesendet. Auf Empfängerseite erkennt die Signtrust-Mail-Software automatisch eintreffende Mails, die signiert oder verschlüsselt sind, überprüft die Signatur und entschlüsselt das Dokument.

› Weitere Trustcenter im Überblick

Die DATEV (http://www.datev.de) hat mit "e:secure" ein vergleichbares Komplettpaket aus Chipkarte mit Signatur und PIN, Signatur-Software und Kartenleser im Programm. Das e:secure-Paket gibt es ausschließlich für DATEV-Mitglieder und deren Mandanten, zum Beispiel Steuerberater und die von ihnen vertretenen Firmen. e:secure ist vornehmlich auf den Einzelarbeitsplatz ausgerichtet.

Die Telekom-Tochter Telesec (http://www.telesec.de) bietet mit ServerPass ein Zertifikat, das ein E-Commerce-Anbieter auf seinem Webserver einbindet. Die Bereitstellung kostet 81,20 Euro, die Gebühr für ein Jahr 174 Euro. Telesec ist vor allem auf Teams spezialisiert.

TC Trustcenter (http://www.trustcenter.de) bietet Signaturen für Privatanwender (TC Private) und für Firmen (TC Certificate) sowie Serverzertifikate an. TC-Private-Zertifikate kosten 31 Euro, Firmenzertifikate 62 Euro pro Jahr. Für ein Serverzertifikat (inklusive SSL-Verschlüsselung) legt man 260 Euro für den ersten Server an, für weitere Server je 130 Euro pro Jahr. Außerdem bietet TC Trustcenter eine Reihe von maßgeschneiderten Paketen für Firmen an, die eine Reihe von Arbeitsplätzen mit digitalen Signaturen

ausstatten wollen.

› Problem Interoperabilität

Das derzeit größte praktische Problem der digitalen Signatur ist die mangelnde Interoperabilität. Damit ist gemeint, dass im Geschäftsverkehr mit den Kunden eines anderen Trustcenters die SmartCards und die Anwendungs-Software nicht beliebig einsetzbar sind.

Im Klartext: Wer Kunde bei Trustcenter x ist, kann mit Kunden von Trustcenter y nicht verschlüsselt kommunizieren. Gründe für die mangelnde Standardisierung sind die unterschiedlichen Implementierungen internationaler PKI-Standards wie PKCS#1 und X.509.

Bislang existierten in Deutschland zwei zueinander inkompatible Spezifikationen für das Management elektronischer Zertifikate: die "Industrial Signature Interoperability Specification" (ISIS) vom Verein AG Trustcenter e.V. (http://www.t7-isis.de) und "MailTrust" von Teletrust e.V (http://www.teletrust.de) . Um die Akzeptanz der digitalen Signatur zu erhöhen, hat das Bundesministerium für Wirtschaft und Technologie (BMWi (http://www.bmwi.de)) den Firmenverbund Teletrust beauftragt, ISIS und MailTrust zusammenzuführen und einen einheitlichen Standard zu erarbeiten. Die Spezifikation des neuen gemeinsamen Standards ISIS-MTT Version 1.0 steht seit Oktober 2001 im Web zur freien Verfügung (http://www.t7-isis.de/ISIS-MTT/isis-mtt.html) .

› Ziel: E-Government

Die Erarbeitung der "vereinheitlichten ISIS-MTT-Spezifikationen für Interoperabilität und Testsysteme" ist der erste Schritt eines mehrstufigen Projekts, in dem bisherige Erfahrungen mit internationalen Standards gekoppelt werden sollen. Die Arbeitsgruppe ruft auf ihrer Website (http://www.t7-isis.de) ausdrücklich zu Kommentaren auf. Anregungen und Vorschläge werden geprüft, die Kommentare veröffentlicht. Noch für das Jahr 2002 sind die Entwicklung und Bereitstellung von Testtools, die Vorbereitung eines Testbeds und Pilotanwendungen des Testbeds geplant, die alle definierten Schnittstellen der ISIS-MTT-Spec enthalten. Hersteller können dann ihre Produkte überprüfen und von einer unabhängigen Prüfstelle abnehmen lassen.

Die Bundesregierung möchte die ISIS-MTT-konformen Signaturen möglichst bald einsetzen. Anwendungsfelder sind die vom BMWi geförderten Pilotprojekte MEDIA@Komm (http://www.mediakomm.net) , Elektronische Wahlen I-Vote (http://www.internetwahlen.de) sowie die Initiative BundOnline 2005 (http://www.bundonline2005.de) . Unter dem Motto BundOnline 2005 will die Bundesregierung alle Internet-fähigen Dienstleistungen des Bundes anbieten. Staatssekretär Dr. Alfred Tacke vom BMWI prophezeit: "Ich erwarte, dass jetzt rasch interoperable elektronische Signaturprodukte für jedermann angeboten werden und dadurch die Akzeptanz von E-Government- und E-Business-Lösungen deutlich erhöht wird. Dies ist ein wesentlicher Schritt für den breiten Durchbruch beim rechtsverbindlichen elektronischen Geschäftsverkehr."

› Praxisbeispiele

Für Privatanwender sind digitale Zertifikate derzeit nicht sehr interessant, weil den jährlichen Kosten von mindestens 25 Euro kaum Nutzungsmöglichkeiten gegenüberstehen. Außer einigen Pilotprojekten zum Thema Behördengang per Internet und der Möglichkeit, E-Mails in Outlook zu verschlüsseln, existieren aktuell keine praktischen Anwendungsmöglichkeiten. Aber ihre Entwicklung ist nur eine Frage der Zeit.

Die meisten Pilotprojekte beschränken den Einsatz der elektronischen Signatur auf sehr einfache Dinge. Beim Städteverbund Nürnberg etwa wird die digitale Signatur im Rahmen einer multifunktionalen Chipkarte für den Online-Antrag von Anwohnerparkausweisen eingesetzt. Der Verbund hat für die Umsetzung mit Curiavant (http://www.curiavant.de) ein eigenes Unternehmen gegründet. Mit dem elektronischen Verwaltungssystem wird den Bürgern der aufwendige Behördengang erspart.

Statt sich persönlich zum zuständigen Beamten zu begeben, Bargeld einzuzahlen und den Ausweis abzuholen, kann der Geschäftsprozess vom heimischen PC aus per

Chipkarte erledigt werden. Die digitale Signatur bürgt dabei für die richtige Identifikation der Person. Da die Karte auch eine integrierte Bezahlfunktion enthält, kann der Antragsteller auch gleich am PC bezahlen. Der Parkausweis kommt dann per Post.



Im Einsatz: Signaturkarte mit Chipkartenleser, wie er beim Projekt Anwohnerparkausweis des Städteverbunds Nürnberg verwendet wird.

Als nächste Anwendung ist eine Einwohnermeldeauskunft geplant. Dabei sollen berechtigte Personen wie Anwälte via Internet Auskünfte einholen können. Auch eine Auskunfts- und Buchungsmöglichkeit bei Volkshochschulen und anderen Bildungsträgern soll bald starten. Interessierte können sich dann über das Internet nicht nur über einzelne Kurse informieren, sondern auch unabhängig von Öffnungszeiten anmelden und die Kurse bezahlen.

› Schröders Chefsache

Auch anderswo wird an kleinen Anwendungen für die digitale Signatur gearbeitet: In Bremen (http://www.bos-bremen.de) sind 15 Geschäftsvorfälle aus Verwaltung und Wirtschaft mit einer elektronischen Signatur nutzbar. Bis Ende 2002 soll diese Zahl auf 70 anwachsen. Dazu werden in den kommenden Monaten 10.000 Bürger mit Chipkarten ausgerüstet. Die Universität Bremen baut derzeit die technische Infrastruktur (http://www.signatur.uni-bremen.de) für den Einsatz der elektronischen Signatur für ihre Studenten auf. Als mögliche Anwendungen werden die An- und Abmeldung zu

Prüfungen, die Nutzung von Bibliotheksdiensten oder die Kommunikation mit dem BAföG-Amt genannt.

Bundeskanzler Schröder hat im Mai letzten Jahres das Thema Digitale Signatur und E-Government zur Chefsache erklärt und die oben erwähnte Initiative BundOnline 2005 ins Leben gerufen. Damit verpflichtet sich die Bundesregierung, alle Internet-fähigen Dienstleistungen (http://www.bundonline2005.de) des Bundes - etwa 1200 an der Zahl - bis zum Jahr 2005 online zu stellen. Seine Vorstellungen entwickelte der Bundeskanzler vor mehr als 200 Behördenleitern auf einer Tagung zur Initiative in Berlin - und machte eine gewagte Prophezeiung: "In ein paar Jahren wird kaum noch jemand Verständnis dafür haben, wenn man Personalausweis oder Führerschein nicht per Internet beantragen kann".

› Fazit

Während die Sache mit der digitalen Signatur juristisch im Lot ist, hat die praktische Umsetzung noch mit Kinderkrankheiten zu kämpfen. Für Privatnutzer gibt es derzeit kaum sinnvolle Anwendungen, Geschäftskunden scheuen die erforderlichen Investitionen und bemängeln die noch schwach ausgebaute Infrastruktur. Mangelhaft sind vor allem die noch spärlich gesäten Trustcenter, die zudem noch wenig Erfahrung mit millionenfacher Nutzung haben. Wird hier ein Fehler begangen, etwa indem ein Betrüger die Signatur für eine gefälschte Identität erhält oder Hacker Zugriff auf die Computersysteme in der Zertifizierungsstelle bekommen, lassen sich die Folgen ausmalen. Sicherheitsexperten bemängeln, dass neben den akkreditierten Zertifizierungsstellen, welche behördlich kontrolliert werden, auch solche ohne Überprüfung zugelassen sind. Die Bundesnotarkammer in Köln empfiehlt deshalb, nur akkreditierte Zertifizierungsdienste zu nutzen.

Größtes Manko für die Ausbreitung der digitalen Signatur waren bislang fehlende Standards, was dazu führte, dass im Geschäftsverkehr mit den Kunden eines anderen Trustcenters die SmartCards und die Anwendungs-Software nicht beliebig einsetzbar sind. Nun hat die Bundesregierung darauf gepocht, die beiden rivalisierenden Spezifikationen für das Management elektronischer Zertifikate zu vereinheitlichen und hofft, dass interoperable Signaturprodukte endlich den Durchbruch für die digitale Unterschrift bringen. Bis zum Jahr 2005 sollen dann alle Internet-fähigen Dienstleistungen des Bundes per elektronischer Signatur und Web verfügbar sein. (ala)

› Weitere Themen zu diesem Artikel:

- Elektronisch unterschreiben (http://www.tecchannel.de/internet/402/index.html)
- Kryptographie-Grundlagen (http://www.tecchannel.de/internet/416/index.html)
- Sicher durch Biometrie (http://www.tecchannel.de/software/824/index.html)

Sicher durch Biometrie

› Biometrische Verfahren wie Fingerabdruck und Gesichtserkennung identifizieren Personen mit hoher Sicherheit. Neben der staatlichen Überwachung sind sie damit auch als Ersatz für Passwörter und PINs geeignet.

› VON DR. KLAUS MANHART

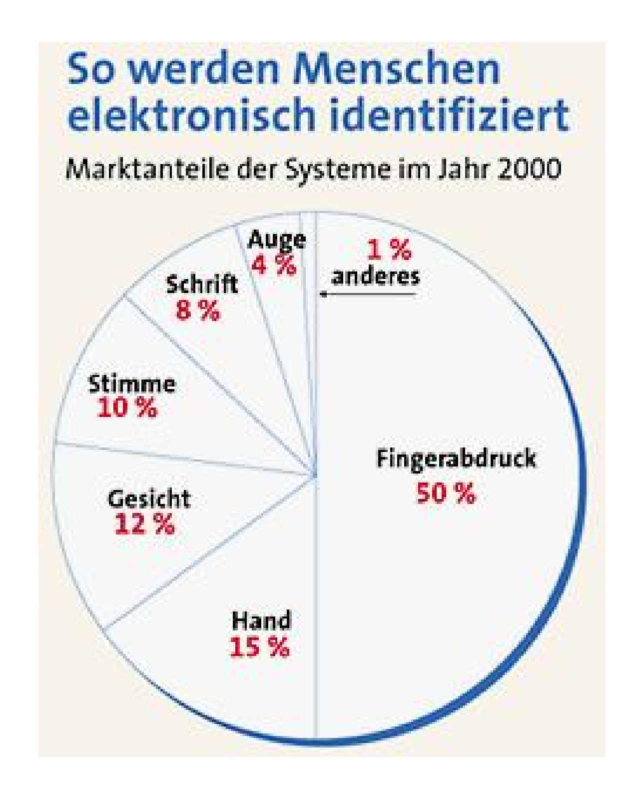
Seit den Terroranschlägen vom 11. September ist die Biometrie in aller Munde. Bislang führte die Sicherheitstechnik für die Erkennung eines Menschen anhand persönlicher Charakteristika ein Schattendasein. Doch jetzt überhäufen Anfragen die Hersteller biometrischer Sicherheitslösungen. Um dem Ansturm Herr zu werden, hat etwa das größte Consulting-Unternehmen für Biometrie-Systeme, die International Biometric Group (http://www.biometricgroup.com/) , die häufigsten Fragen und Antworten im Internet veröffentlicht.

Stark interessiert an biometrischen Erkennungssystemen ist vor allem die Flugindustrie. Insbesondere amerikanische Fluglinien und Airports fordern nach den verheerenden Attentaten die Einführung biometrischer Technologien. So verlangt die Air Transport Association (http://www.aviationnow.com/avnow/news/channel_comm.jsp?view=story&id=news/cbio1110.xml) (ATA), die Vereinigung der US-Airlines, von der Regierung die Einführung einer Identitätskarte mit biometrischen Erkennungsmerkmalen wie Fingerabdrücken. Der Flughafen in Oakland im Bundesstaat Washington wird gerade als einer der ersten mit einer automatischen Gesichtserkennung ausgestattet. Eine Videokamera erfasst Personen und vergleicht die gesichtsspezifischen Merkmale mit gespeicherten Daten in einer zentralen Datenbank.

In Deutschland will Innenminister Schily Pässe und Personalausweise um biometrische Merkmale bereichern. Das so genannte "zweite Sicherheitspaket" oder "zweite Anti-Terror-Paket" der Bundesregierung (http://www.bundesregierung.de/frameset/index.jsp) soll zahlreiche Sicherheitsgesetze sowie ausländerrechtliche Vorschriften anpassen. Der Entwurf für das Pass- und Personalausweisrecht sieht vor, dass neben dem Lichtbild und der Unterschrift biometrische Merkmale aufgenommen werden dürfen. Ob die Personalpapiere in Zukunft tatsächlich die Daten von Fingerabdrücken, Augenhintergründen, ganzen Händen oder Gesichtern enthalten, steht noch nicht fest.

› Vor- und Nachteile der Biometrie

Dass gerade die Biometrie von der gegenwärtigen Sicherheitshysterie profitiert, hat einen handfesten Grund: Biometrische Verfahren bieten im Vergleich zu anderen Systemen wie Kennwörtern ein Mehr an Sicherheit. Sie beruhen auf der Annahme, dass Personen eindeutige unveränderliche Merkmale besitzen, die sich zur Identifikation mit Hilfe elektronischer Verfahren nutzen lassen. Zu diesen Merkmalen gehören Fingerabdrücke, die menschliche Stimme, die handschriftliche Unterschrift oder Aufnahmen des Augenhintergrundes. Einen kurzen Überblick über die einzelnen Verfahren und ihre Vor- und Nachteile finden Sie auf der Seite "Biometrische Verfahren im Überblick" am Ende des Artikels.



Marktanteile: Von allen biometrischen Verfahren hat der Fingerprint die mit Abstand größte Marktbedeutung. (Quelle:Biometric Industry Report)

Der wesentliche Vorteil der Biometrie: Sie erfasst mit physiologischen oder verhaltenstypischen Charakteristika personengebundene und nicht nur - wie bei PIN und Passwort - personenbezogene Merkmale. PIN und Passwort kann man an eine andere Person weitergeben, biologische Eigenschaften nicht. Ein Körpermerkmal ist einzigartig auf der Welt. Der Besitzer kann es weder verlieren noch vergessen. Der Körper selbst wird zum Ausweis, zum biologischen Kennwort.

Biometrische Verfahren bieten folgende Vorteile

- Biometrische Merkmale können weder verloren gehen noch an andere Personen weitergegeben werden
- Die Fälschungssicherheit ist extrem hoch
- Die Gültigkeitsdauer ist extrem lang
- Die Kosten für den langfristigen Betrieb sind gering

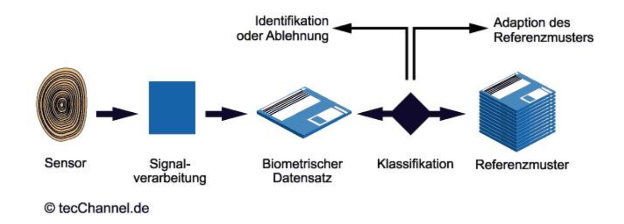
Dem stehen aber auch Nachteile gegenüber:

- Die Kosten für die erstmalige Beschaffung und Einrichtung von biometrischen Systemen sind relativ hoch
- Es gibt hygienische Bedenken bei berührungssensitiven Systemen
- Der Persönlichkeitsschutz ruft vielerorts Gegner und Kritiker dieser Systeme auf den Plan
- In der Praxis tauchen oft Probleme auf, wenn die biometrischen Merkmale gestört sind: Kleinigkeiten wie Schwielen, Blasen, Verletzungen oder Ähnliches stellen beispielsweise ein Gerät zur Erkennung der Handgeometrie vor echte Schwierigkeiten.

› Grundprinzip der Computer-Erkennung

Alle biometrischen Messverfahren funktionieren nach dem demselben Grundprinzip: Vor der biometrischen Autorisation lernt das System den Benutzer kennen, indem es seine

Merkmalstruktur analysiert - den Vorgang nennt man Personalisierung oder Enrollment. Die Analyse erzeugt ein biometrisches Muster von dem zu identifizierenden Merkmal: Scanner und Computer vermessen hierzu Gesicht, Iris, Stimme, Finger oder die ganze Hand. Das System speichert nicht komplette Bilder, sondern nur ausgewählte Merkmale. Die auf das Wesentliche reduzierten Messergebnisse werden als so genannte Templates auf einem Server oder einer Smartcard abgelegt. Das Template dient künftig als Vergleichsmuster, wann immer der Mensch sich per Fingerabdruck oder Stimme ausweisen soll.



Erkennung: In der Enrollmentphase wurde der biometrische Datensatz generiert und als Referenzmuster gespeichert. In der Überprüfungsphase vergleicht der Rechner den aktuellen Datensatz mit dem gespeicherten Muster.

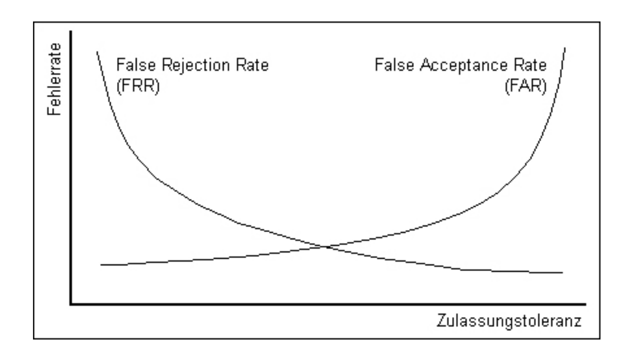
Bei der Überprüfungsphase läuft bis zur Bildung des Referenzdatensatzes der gleiche Vorgang ab. Anschließend existieren zwei weitere Vorgehensweisen, die Verifikation und die Identifikation. Bei der Verifikation (Authentisierung) gleicht man das aktuelle Merkmal mit einem vorher aufgenommenen Merkmal (1:1-Vergleich) ab. Der Benutzer gibt sich vorher gegenüber dem System zu erkennen, zum Beispiel durch die Eingabe einer Benutzerkennung. Anschließend wird ihm vom System das bei der Personalisierung gespeicherte Referenzmuster zugeordnet. Dieses Verfahren erfordert nur eine geringe Rechenleistung.

Bei der Identifikation hingegen erfolgt der Abgleich der aktuell aufgenommenen Merkmale gegen alle vorliegenden Daten (1:n-Vergleich). Das System ermittelt den Benutzer selbstständig. Je nach Menge der gespeicherten Referenzdaten dauert die Identifikation sehr lange. Benutzerfreundlichkeit und Anwendbarkeit sind dadurch erheblich eingeschränkt.

› Fehlersicherheit

Trotz der fortgeschrittenen Technologie ist kein biometrisches Verfahren zu 100 Prozent sicher. Gute Systeme identifizieren Menschen heute mit einer Fehlerquote von unter 10 Prozent. Das Problem dabei: Bei zwei Messungen mit dem Computer liefern Finger, Auge oder Unterschrift nie exakt die gleichen Daten. Die Übereinstimmung lässt sich nur ungefähr feststellen.

Zudem unterliegen viele biometrisch erfassbaren Merkmale einem Veränderungsprozess. Krankheiten, bestimmte Lebensumstände oder einfach der Alterungsprozess verändern biometrische Eigenschaften. Bei der Umsetzung von Iris-Daten kann es Schwierigkeiten geben, wenn der Ausweisinhaber an Diabetes erkrankt und sich seine Augen verändern. Bei der Gesichtserkennung müsste bei der Aufnahme in einen Pass beachtet werden, dass die Anschaffung einer neuen Brille viele Messpunkte verändert. Trotz dieser widrigen Umstände ermöglichen gute biometrische Verfahren eine hohe Wiedererkennungsrate, vorausgesetzt, das System wird häufig genutzt und passt das interne Referenzmodell nach jeder Erkennung dynamisch an.



Genau oder sicher: Wer zu scharf überprüft, weist oft auch berechtigte Benutzer ab. (Quelle: TÜV Nord Security)

Eine wichtige statistische Größe für die Erkennungsgenauigkeit biometrischer Systeme ist die False Accept Rate (FAR). Sie gibt die Häufigkeit an, mit der nicht berechtigten Personen Zugriff gewährt wird. Das Gegenstück zur FAR ist die False Reject Rate (FRR). Sie beschreibt, wie häufig berechtigte Personen vom System zurückgewiesen werden. Je kleiner die FAR wird, desto höher wird die FRR. Bei der Konfiguration eines Systems muss darauf geachtet werden, dass beide Werte im optimalen Verhältnis zueinander stehen. Dabei handelt es sich um einen empirischen Wert, der nur durch Tests herausgefunden werden kann.

› Biometrie in der Wirtschaft

100-prozentige Sicherheit kann man sich von biometrischen Verfahren nicht erwarten. Ob biometrische Kontrollen die Terroranschläge verhindert hätten, muss bezweifelt werden. Um verdächtige Personen zu erkennen, muss zumindest ein Referenzmuster vorhanden sein - islamistische Schläfer, die bislang nie negativ in Erscheinung traten, hätten biometrische Systeme nicht herausfiltern können.

Ohnehin dürfte das Haupteinsatzgebiet biometrischer Systeme nicht im staatlichen Sicherheitsbereich liegen sondern in der Wirtschaft. Doch Firmen reagieren noch zögerlich beim Einsatz biometrischer Systeme. Hohe Fehlerquoten, teure Preise und die komplizierte Installation der Systeme waren aus Sicht von Branchenkennern bislang die Hauptgründe für die mangelnde Akzeptanz. Die US-Organisation der Biometrie-Anbieter IBIA (http://www.ibia.org) rechnet erst für 2010 mit einem signifikanten Markt, der in den USA bei 1 bis 2,5 Milliarden Dollar liegen soll - die Prognose erfolgte allerdings vor dem 11. September. Optimistischer sind die Vorhersagen von Frost & Sullivan. Das Marktforschungsinstitut prognostiziert weltweit schon im Jahr 2006 ein Marktvolumen von 1,6 Milliarden Dollar.

Wirtschaftliche Anwendungsgebiete biometrischer Identifikationsverfahren reichen von der Identifizierung von Personen in einem überwachten Raum bis zur Zugangskontrolle für Hochsicherheitsräume oder Geldautomaten. Darüber hinaus dienen biometrische Verfahren im Zusammenhang mit der Abgabe von Willenserklärungen im elektronischen Rechtsverkehr. Bei der digitalen Signatur von Dokumenten kommt zur Freischaltung des privaten Schlüssels - und somit als Zugangsberechtigung zur Erzeugung der Signatur - anstatt einer PIN ein biometrisches Merkmal zum Einsatz.

Den Wildwuchs an Passwörtern und Codes los zu werden könnte einer der wichtigsten Motiviationsgründe sein, warum die Industrie um biometrische Verfahren nicht umhin kommt. Denn hier ist das Chaos perfekt: Je eine mehrstellige Zahl für EC- und Kreditkarte, Mobiltelefon, Anrufbeantworter, Transaktionsnummern für das Homebanking und mehrere Passwörter - wer kann hier noch die Übersicht behalten? Die Zahleneingabe ist nicht nur umständlich und unhandlich. Die Codes können leicht ausgespäht und - beabsichtigt oder unbeabsichtigt - weitergegeben werden. Und die Inflation der Geheimnummern führt unweigerlich auch dazu, dass man sie immer öfter vergisst. Laut einer Studie von Morgan Keegan & Co. entstehen im Zusammenhang mit vergessenen Passworten und PINs Kosten von 100 - 200 Dollar pro Benutzer und Jahr.

Hersteller von Biometrie-Systemen haben damit ein gutes Argument für die Wirtschaft in der Hand: "Biometrische Verfahren sind in der IT-Welt auch aus wirtschaftlichen Gründen hochinteressant", sagt Norbert Pohlmann, Marketing-Vorstand des Security-Anbieters

Utimaco Safeware. "Durch die Einsparung der Support-Kosten für vergessene Passwörter und PINs machen sich Investitionen in Biometrie - abgesehen vom Hinzugewinn an Sicherheit - schnell bezahlt".

› Zugang per Fingerabdruck

Als Zugangsidentifikation für Computersysteme und im Mobilbereich bei Notebooks, PDAs, Handys und Autos kommt der Fingerabdruck in Frage - das am weitesten verbreitete biometrische Verfahren. Statt Passwort und PIN gewährt der Fingerprint nur Nutzern mit den korrekten Fingerrillen den Zugang. Da jeder Fingerabdruck einzigartig ist, beweist er mit extrem hoher Wahrscheinlichkeit die Identität des Benutzers. Ein Handy-Nutzer etwa, der jedes Telefonat mit seinem Fingerabdruck bestätigt, kann das Mobiltelefon überall liegen lassen, ohne dass ein Fremder damit telefonieren kann. Eine Übertragung des Fingerprints an andere Personen ist ausgeschlossen, selbst eineiige Zwillinge besitzen nicht den gleichen Fingerabdruck.

Beim Fingerprint scannen Sensoren Linienverläufe, Wirbel, Schlingen und Verzweigungen des Fingerabdrucks, die so genannten Minuzien. Zwölf dieser Merkmale reichen aus, um den Fingerabdruck einem Menschen eindeutig zuordnen zu können. Das Template ist entweder direkt im Gerät gespeichert, liegt zentral auf einem Server oder auf einer SmartCard. Stimmen die Werte nicht überein, wird der Zugang verweigert.

Selbst wer versucht, das Sensorsystem mit einem Wachsabdruck oder gar einem amputierten Finger zu überlisten, kommt bei hochwertigen Fingerprintsystemen nicht zum Zuge. Zusätzliche Sensoren, die in das Lesegerät integriert sind, messen den Puls im Finger und können so einen echten Fingerabdruck von der Fälschung unterscheiden.



Fingertip-Sensor: Die Identifikation erfolgt über den Fingerabdruck, der von der Oberfläche eines Mikrochips erfasst wird.

Die Sensoren zeichnen sich durch geringe Stromaufnahme bei niedriger Betriebsspannung und hoher mechanischer Stabilität aus. Sie sind darüber hinaus relativ unempfindlich gegen Verschmutzung und Fremdlichteinstrahlung, ein Vorteil gegenüber optischen Systemen. Damit gehört der Fingerabdruck zu den einfachsten und effektivsten biometrischen Erkennungsmethoden.

› Fingerabdruck - Anwendungsbeispiele

Die Firma Siemens ist in Deutschland im Bereich Fingerabdruck-Erkennung (http://www.fingertip.de) führend. Schon 1997 begann die Entwicklung des Sensors. Die Grundidee dahinter: Wenn ein Finger auf die 1,7 cm² große Chipfläche gelegt wird, erfassen über 65.000 kapazitive Sensorelemente mit einer Auflösung von 500 dpi die Entfernung der Haut von der Chipoberfläche. Das Bild der Fingerkuppe mit allen Merkmalen wie Linienenden, Verzweigungen und Wirbeln leitet der Sensor an einen Rechner weiter. Der wiederum extrahiert daraus ein bis zwei Dutzend charakteristischer Stellen und vergleicht sie mit den gespeicherten Originaldaten.



Sicher ist sicher: Eine Fingerprint-ID-SmartCard ist eine Anwendung des Siemens Fingertipp-Sensors.

Konkret verwendet wird der Sensor seit Jahren bei der ID-Maus. Der Nutzer kann sich mit einem kurzen Fingertipp auf den Sensor der Maus identifizieren. Die Siemens ID Mouse unterstützt nicht nur die Anmeldung am lokalen PC, sondern kann mit Hilfe einer speziellen Software auch einfach in Netzwerke eingebunden werden. Die biometrischen Referenzdaten erlauben eine automatische Freischaltung aller Ressourcen, auf die ein Anwender Zugriff hat, verknüpft werden. Dies gilt für Unternehmensnetze bzw. Intranets wie auch für das Internet. Für hohe Sicherheitsanforderungen sorgt eine optionale Kombination aus ID Mouse und SmartCard.



Siemens ID-Mouse: Sie identifiziert den Nutzer mit einem kurzen Fingertipp auf den Sensor der Maus.

Die ID-Mouse ist für 179 Mark unter anderem im Online-Shop (http://www.siemens.de/idmouseshop) von Siemens erhältlich. Eine Erweiterung der Fingerprint-Maus ist die optische Variante für 230 Mark, die ID Mouse Professional. Sie bietet ein zusätzliches Feature: Das Plug-in BioProtect verschlüsselt Microsoft-Office-Dokumente. Ein Klick auf das Icon und ein kurzes Auflegen eines Fingers auf dem Sensor der ID Mouse Professional genügen, damit Word-, Excel- und Access-Dokumente verschlüsselt (Triple-DES) auf der Festplatte des PCs gespeichert sind. Öffnen und entschlüsseln lassen sich die Dokumente ebenfalls wieder per Fingerabdruck. Siemens will Besitzern der ID Mouse Professional das Plug-in in Kürze kostenlos zur Verfügung (http://www.siemens.de/biometrie) stellen.

Auf der Systems hat Siemens Biometrics außerdem ein Software-Entwicklungspaket vorgestellt, das es der Linux-Gemeinde erlaubt, die ID Mouse Professional in Linux-Anwendungen zu integrieren. Damit genügt künftig auch unter Linux ein Fingerabdruck, um Transaktionen zu bestätigen oder um sich zu authentifizieren.

› Weitere Anwendungsbeispiele

Fingerabdruck-Sensoren mit entsprechender Authentifizierungs-Software finden sich auch in Notebooks wie dem Acer (http://www.acer.de) Travelmate 739TLV. Der Sensor ist dabei in die Handauflage des Travelmate-Notebooks integriert. Beim Erscheinen der Log-in-Aufforderung legt der Benutzer einfach seinen Finger auf den Sensorchip. Ohne Freigabe durch den Fingerabdruck eines autorisierten bootet das Notebook nicht und ist damit unbrauchbar. Auch beim Ausbau der Festplatte eines gestohlenen Travelmate 739TLV verhindert die Authentifizierungs-Software das Lesen des verschlüsselten Laufwerks in einem anderen.



Sichere Daten: Das Acer Travelmate Notebook 739TLV erkennt den Nutzer über den Fingerabdruck.

Einen Fingerprint-Sensor mit Smartcard hat die Firma Utimaco (http://www.utimaco.de) im Programm. SafeGuard Biometrics von Utimaco ermöglicht die Integration von Biometrie in komplexe IT-Sicherheitsanwendungen. Die Lösung besteht aus einem kombinierten Fingerabdruck-Smartcard-Leser, einer biometriefähigen RSA-Smartcard, einer Software zur Erfassung von Fingerabdrücken sowie einer biometrischen Log-on-Erweiterung (BioGINA). Das spezielle Match-on-Card-Verfahren ermöglicht die Prüfung des Fingerprints gegen das zuvor ermittelte Referenzmuster direkt auf der Smartcard. Der Fingerabdruck kann auf diese Weise bestehende Smartcard-PIN-Absicherungen vollständig ersetzen.



Doppelt gesichert: SafeGuard Biometrics von Utimaco besteht aus einem kombinierten Fingerabdruck-Smartcard-Leser.

In der Grundausstattung ermöglicht das Produkt eine biometrische Zugangskontrolle zum PC mit Arbeitsplatzsperre bei gezogener Smartcard. Die auf der Smartcard gespeicherten Passworte, Schlüssel und Zertifikate können für weitere Single-Sign-on-Prozesse im Netz, für transparente Dateiverschlüsselung, für die digitale Signatur von E-Mails und Dokumenten sowie für Virtual Private Networks (VPN) genutzt werden.

› Erkennung von Gesicht und Stimme

Aufwendiger und teurer als die Fingerscan ist die Gesichtserkennung. Bei zusätzlicher Auswertung von Bewegungen, beispielsweise der Lippen, bietet sie eine hohe

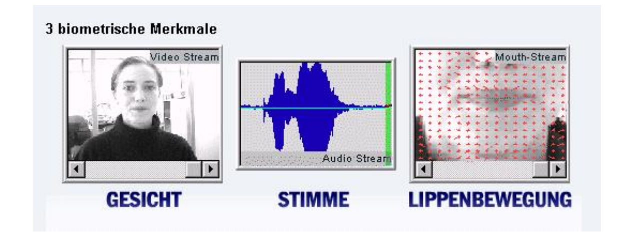
Erkennungszuverlässigkeit.

Die Gesichtserkennung hat sich vor allem als Zugangskontrolle für Mitarbeiter in Unternehmensnetzen bewährt. Die zu identifizierende Person muss ein bestimmtes Wort in die Kamera sprechen. Spezielle Algorithmen reduzieren die Bilder auf die wesentlichen Erkennungsmerkmale. Zur Analyse der Lippenbewegung wird eine Folge von Teilbildern der Mundpartie zu je 128 x 128 Pixeln extrahiert. Ein Algorithmus ermittelt den optischen Fluß aus jeweils zwei aufeinanderfolgenden Bildern und speichert ihn in 16 Feldern zu je 32 x 32 Vektoren. Optional kann man die Wellenform des gesprochenen Wortes mit einer zuvor aufgenommenen Wellenform vergleichen. Durch die Kombination mehrer Körper- und Verhaltensmerkmale erhöht sich die Sicherheit deutlich.

Das System BioID (http://www.bioid.de) der gleichnamigen Firma, ursprünglich vom Fraunhofer-Institut entwickelt, identifiziert den Nutzer anhand der Gesichtsform. Zusätzlich bezieht das System Stimme und Lippenbewegung ein. Jedes Merkmal wird einzeln, aber parallel ausgewertet. Um erkannt zu werden, blicken die Benutzer in die Kamera und nennen beispielsweise ihren Namen. Innerhalb von 1,5 bis 2 Sekunden werden die drei sich ergänzenden biometrischen Merkmale analysiert.

› Kombinationen funktionieren auch bei Erkältung

Durch Nutzung von drei Kriterien in einem integrierten Authentisierungsvorgang verkraftet BioID die täglichen Abweichungen von der Mustervorlage, beispielsweise wenn die Stimme auf Grund einer Erkältung heiser klingt. Damit kommt es wesentlich seltener zu irrtümlichen Abweisungen. An Hardware benötigt das Erkennungssystem eine standardmäßige PC- oder Videokamera und ein Mikrofon. Bei der Ersterkennung fordert BioID auf, in die Kamera zu sehen und dabei einen Erkennungstext zu sagen. Der davon abstrahierte Datensatz, den BioID aus der Aufnahme erzeugt, wird verschlüsselt und auf einem gesicherten Server oder einer Smart Card abgelegt.

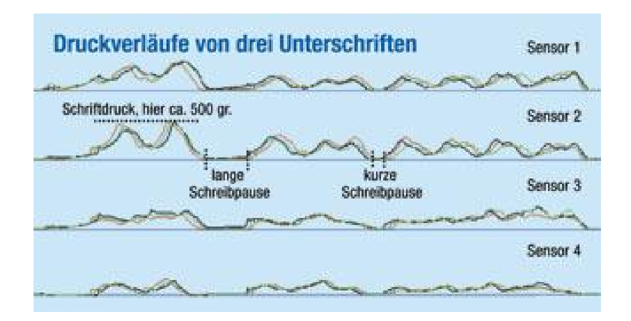


Kombination: Neben Gesichtserkennung bezieht BioID auch Stimme und Lippenbewegungen in die Analyse ein.

"Bei mittleren bis großen Einrichtungen muss der Authentisierungsvorgang für Administratoren und Endanwender möglichst einfach gehalten werden", erklärt Dr. Robert Frischholz, Director R&D von BioID. "Bei der biometrischen Authentisierungslösung BioID erfolgt die Analyse bereits nach einmaliger Vorlage der Merkmale." BioID gibt es in verschiedenen Versionen. Als reiner Client auf einem PC, als Client-Server - wobei der Client den biometrischen Datensatz erhebt und an den Server weiterleitet, als Türsicherung und als Set von Software-Modulen für unternehmensspezifische Projektanforderungen.

› Unterschriftenerkennung via Schreibdruck

Auch die Unterschrift kann man zur Autorisierung nutzen. Dabei wird allerdings nicht - wie viele vermuten würden - das Schriftbild analysiert, sondern das dynamische Schreibverhalten des Nutzers. Druck und Geschwindigkeit sind zwei Parameter, die hier zum Einsatz kommen. Sensoren messen die Kräfte und Beschleunigungen, die bei der Bewegung des Stiftes auftreten. Daraus ermittelt eine Auswertlogik die individuellen Merkmale der Unterschrift.



Mit Schwung: Bei der Unterschriftenerkennung werden Unterschriften und andere eigenhändig geschriebene Texte nicht auf Grund ihrer sichtbaren Anteile, sondern anhand der unsichtbaren Anteile wie Druck auf Echtheit überprüft.

Ein biometrisches System zur Unterschriftenerkennung, mit dem rechtsverbindliche Unterschriften möglich sind, ist Hesy (http://www.hesy.de) . "Hesy kombiniert das in der IT-Sicherheit seit langem bekannte Passwort mit dem biometrischen Merkmal der Unterschrift und bietet damit gegenüber Zahlencodes einen entscheidenden Vorteil: Die Unterschrift als aktive Willenserklärung des Nutzers ist fälschungssicher", erklärt Hesy-Entwickler Rene Baltus.

Das patentierte Verfahren basiert auf der Messung des Schreibdrucks. In ein Schreibtableau integrierte Drucksensoren erfassen die mit einem herkömmlichen Stift geleistete Unterschrift. Aus der Information der Schreibdynamik werden Stiftposition, Druckstärke, Länge, Breite, Schriftwinkel und Zeitverlauf der Unterschrift errechnet und in Echtzeit verglichen. Die benötigten Referenzdaten sind auf einem PC, einem Notebook oder transportabel auf einer SmartCard gespeichert. Die Referenzdaten können öffentlich bekannt sein, da es sich bei der Unterschrift um ein aktives (dynamisches) biometrisches Merkmal handelt.

Die Anwendung für die Nutzer ist einfach und bequem: Ein Papier, das auf dem Signatur-Tablett liegt, wird wie gewohnt unterschrieben. Das Tablett unter dem Papier erfasst die Unterschrift und leitet die Daten an einen PC weiter .



Druckempfindlich: Hesy ist ein elektromechanisches Unterschriftentablett, das den Schreibdruck mittels mehrerer Drucksensoren analog aufnimmt. Die Drucksensoren befinden sich direkt unterhalb der Schreibfläche - es kann daher mit beliebigen Schreibstiften geschrieben werden

Das System bietet einen unschlagbaren Vorteil, so Baltus. "Wir Menschen müssen nicht umlernen und uns der Technologie anpassen. Wir können das tun, was wir schon seit Generationen tun, um unseren Willen rechtsverbindlich zu dokumentieren: Wir unterschreiben einfach."

› Fazit

Biometrische Verfahren basieren darauf, dass jeder Mensch über einzigartige, nicht kopierbare Körper- und Verhaltensmerkmale verfügt. Biometrisch auswerten lassen sich eine ganze Reihe von Daten: Das Tippverhalten an einer Tastatur, die Fingergeometrie, die Stimme, das Gesicht, die Unterschriftendynamik, das Netzhaut- und das Irismuster oder der Fingerabdruck.

Noch steckt der Markt für biometrische Erkennungssysteme in den Kinderschuhen. Die veränderte Sicherheitslage könnte ihn aber schon bald zum Boomsektor der IT- und Security-Industrie hochpushen. Studien zufolge soll sich der Biometrie-Markt bis zum Jahr 2006 verfünffachen, mit dem derzeit wichtigsten biometrischen Verfahren, dem Fingerprint, soll die Hälfte aller Umsätze erzielt werden.

Der große Vorteil biometrischer Daten: Sie können nicht wie PINs ausgetauscht oder ausgespäht werden. Die Entschlüsselung sensibler Dokumente ist nur noch durch die dazu berechtigte Person möglich. Neben dem staatlichen Sicherheitssektor sollen biometrische Systeme im wirtschaftlichen Bereich die lästigen PINs und Passwörter ersetzen und so mehr Komfort bringen und Kosten sparen.

Bislang haben die Kosten und hohe Fehlerquoten eine schnellere Einführung biometrischer Verfahren blockiert. Die Fehleranfälligkeit beträgt derzeit bis zu 10 Prozent, im günstigsten Fall immer noch 1 bis 5 Prozent. Angesichts der Gelder, die derzeit in die Technologie gesteckt werden, dürfte sich diese Fehlerquote künftig aber deutlich verbessern. (ala)

› Biometrische Verfahren im Überblick

Verfahren	Erläuterung	Vor-/Nachteile
Hand	Geräte erfassen die Abmessungen der Finger und die Dicke der Hand oder liefern auch ein Venenbild.	Vorteil: schon seit mehr als zehn Jahren im Einsatz. Nachteil: Die geometrischen Abmessungen von menschlichen Händen unterscheiden sich nicht genügend
Netzhaut (Iris)	Die Struktur der Augennetzhaut wird mittels eines ungefährlichen Laserstrahls abgetastet	Vorteil: sehr fälschungssicher und niedrige Falscherkennungsraten von bis zu 1 zu 1.000.000. Nachteil: Ängste der Benutzer, die Augen mittels Laser abtasten zu lassen
Fingerabdruck	Fingerabdrücke sind von Mensch zu Mensch unterschiedlich und eigenen sich hervorragend zur physiologischen Erkennung	Vorteil: sehr fälschungssicher und niedrige Falscherkennungsraten von bis zu 1 zu 1.000.000; im Bankenbereich beruhen schon heute 68 Prozent der Biometrie-Anwendungen auf dem Fingerabdruckverfahren. Nachteil: durch den allgemein bekannten Einsatz bei der Polizei bei der Verbrecherjagd große Hemmnisse bei den Benutzern hinsichtlich der Persönlichkeitsrechte
Gesicht	Erkennung erfolgt auf den persönlichen Gesichtsmerkmalen	Vorteil: völlig berührungsfrei. Nachteil: umfangreiche Datensätze

		erfordern schnelle und teure Systeme. Da das System auch zur Erkennung und Identifikation von Personen in der Öffentlichkeit angewandt werden kann, gibt es auch datenschutzrechtliche Probleme
Unterschrift	Erkennung der charakteristischen Unterschriftenmerkmale wie Dynamik des Schreibstiftes	Vorteil: wird vom Benutzer akzeptiert. Nachteil: Problem der Trennung variabler und invarianter Teile bei der Erkennung, hoher Zeitbedarf
Stimme	Spektralanalyse eines (meist vorbestimmten) gesprochenen Wortes	Vorteil: wird vom Benutzer akzeptiert. Nachteil: Problem der Trennung variabler und invarianter Teile bei der Erkennung sowie hoher Zeitbedarf

Quelle: Firstsurf

› Weitere Themen zu diesem Artikel:

Elektronisch unterschreiben (http://www.tecchannel.de/internet/402/index.html)
Bezahlen im Internet (http://www.tecchannel.de/internet/394/index.html)
HBCI - Der neue Homebanking-Standard (http://www.tecchannel.de/internet/62/index.html)
Kryptographie-Grundlagen (http://www.tecchannel.de/internet/416/index.html)

Sichere E-Mail

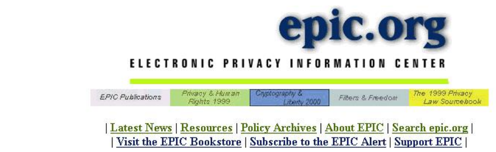
› Die wenigsten Benutzer hegen Bedenken, dass Unberechtigte ihre E-Mails mitlesen könnten. Dabei lauert diese Gefahr auf dem gesamten Übertragungsweg. Doch es gibt wirkungsvolle Schutzmaßnahmen.

› VON ULLI EIKE

Gefährdet ist die Privatsphäre besonders in Firmennetzen (http://www.tecchannel.de/internet/288/index.html) , die mit internen Mailprogrammen arbeiten und alle ein- und ausgehenden Mails zentral über einen Server abwickeln. Es ist kein Geheimnis, dass fast alle leistungsfähigen Mailserver-Programme die Option bieten, eine Kopie der gesendeten und empfangenen Mails zu speichern. Das gibt jedem, der auf den Mailserver Zugriff hat, die Gelegenheit, in aller Ruhe die womöglich private Korrespondenz der Benutzer zu lesen.

Zwar vermittelt die reine Menge der täglich gesendeten E-Mails den Eindruck, das Risiko, ausspioniert zu werden, sei relativ gering. Ein Feature der Mailserver erlaubt es aber, den Postverkehr nach bestimmten Schlüsselbegriffen zu durchsuchen und beim Auftreten eines dieser Wörter die Weiterleitung der Mail zu verweigern, eine Kopie anzulegen und/oder den Postmaster zu benachrichtigen. Insofern ist es sowohl für ein Unternehmen als auch für einen Internetprovider ein Leichtes, die Inhalte von Mails zu kontrollieren und bestimmte Inhalte aufzuspüren

Ein weiteres Problem bei E-Mails ist die Authentizität des Absenders, denn Mailadressen lassen sich leicht fälschen. Schutz bieten unabhängige Zertifizierungsstellen, die mit einem Zertifikat - einer Art digitalem Personalausweis - die Identität des Absenders sicherstellen. Zahlreiche Informationen rund um den Datenschutz finden Sie bei Epic.org (http://www.epic.org) .



Datenschutz: Das Electronic Privacy Information Center (Epic) ist zentrale Anlaufstelle für Informationen rund um Sicherheit und Schutz der Privatsphäre.

Lesen Sie im Folgenden, wie Sie Risiken beim Mailversand ausschalten können und welche Hilfsmittel dazu nötig sind.

› E-Mails verschlüsseln

Wenn Sie vermeiden wollen, dass ein neugieriger Mitmensch Ihre Mitteilungen liest, ist die sicherste Methode die Verschlüsselung. Im Normalfall ist dann nur der Empfänger in der Lage, die Botschaft zu entschlüsseln. Dies ist gleichzeitig auch ein wirksamer Schutz gegen die Filterfunktion der Mailserver, die in dem verschlüsselten Code keine Möglichkeit mehr hat, Suchbegriffe aufzustöbern.

Zum Verschlüsseln einer E-Mail gibt es mehrere Möglichkeiten, die sich in erster Linie durch die Art des Einsatzes und die Stärke der Verschlüsselung unterscheiden. Am

komfortabelsten für den Anwender ist die Integration einer Verschlüsselungsroutine in den täglich benutzten E-Mail-Client. Wer seine Mail browserbasiert direkt aus dem Internet verschickt, findet auch bei einigen kostenlosen E-Mail-Diensten (http://www.tecchannel.de/internet/87/index.html) Features zum Verschlüsseln von Mail. Allerdings werden hier die Daten auf dem Weg zum Webmailer unkodiert und damit auch ungesichert übertragen.

Populärer und sehr beliebt sind externe Programme, wie etwa Pretty Good Privacy (PGP). Sie bieten eine hohe Sicherheitsstufe und genießen nicht zuletzt durch ihre Wurzeln in der Forschung und die Verfügbarkeit des Quellcodes einen guten Ruf.

Auf den nächsten Seiten finden Sie weiterführende Informationen zu den jeweiligen Optionen sowie einen Überblick über essenzielle Grundlagen der Verschlüsselung, ihren Einsatz und die resultierende Sicherheit.

› Verschlüsselungsgrundlagen

Zum Ver- und Entschlüsseln einer Nachricht werden gewöhnlich zwei unterschiedliche Schlüssel eingesetzt (asymmetrische Kryptografie). Die Schlüssel sind voneinander abhängig, lassen sich jedoch nicht aus dem jeweils anderen Schlüssel rekonstruieren. Der Schlüssel, den der Anwender zum Kodieren einsetzt, kann deshalb bedenkenlos öffentlich verteilt werden. Man bezeichnet ihn daher als Public Key.

Zum Entschlüsseln der Nachricht benötigt man den zugehörigen privaten Schlüssel (Private Key). Diesen sollte der Besitzer keinesfalls aus der Hand geben und sicher aufbewahren.

Eine große Gefahr besteht bei diesem Verfahren durch gefälschte Public Keys. Wenn Spion A beispielsweise eine Public-/Private-Kombination erzeugt und den Public Key unter dem Namen von Anwender B veröffentlicht, wird ein weiterer Anwender C möglicherweise bedenkenlos diesen gefälschten Schlüssel für eine vertrauliche Nachricht an B benutzen. Diese ist dann für Spion A, der den zugehörigen Private Key besitzt, lesbar. Öffentliche Schlüssel lassen sich deshalb durch neutrale Stellen zertifizieren, um die Herkunft zu garantieren.

Public- und Private-Key-Verfahren basieren auf so genannten One-Way-Funktionen. Das sind mathematische Funktionen, die sich leicht in eine Richtung berechnen lassen, deren Umkehrung aber nur unter größten Anstrengungen zu berechnen ist. Die bei der Verschlüsselung eingesetzten One-Way-Funktionen lassen sich jedoch zurückberechnen, sobald zusätzliche Informationen zur Verfügung steht. Diese Teilinformation (Trap-Door) sind im Private Key enthalten und ermöglichen es, die mit dem Public Key verschlüsselte Nachricht wieder zu entschlüsseln.

Tatsächlich ist es mathematisch extrem schwer, zu beweisen, dass eine Funktion wirklich nur in eine Richtung leicht zu berechnen ist. Alle derzeit eingesetzten Public-Key-Verfahren benutzen Funktionen, von denen man lediglich annimmt, dass sie schwer rückübersetzbar sind. Sollte es eines Tages gelingen, ein Verfahren zu entwickeln, welches bei einer solchen Funktion ohne die Trap-Door auskommt, würden sämtliche mit dem betreffenden Public Key verschlüsselten Nachrichten von einem Moment zum anderen ihren Schutz verlieren.

› Algorithmen en detail

Pretty Good Privacy beispielsweise benutzt vier verschiedene Verschlüsselungsalgorithmen, um die Nachricht zu sichern: IDEA/3DES und RSA/ElGamal, wobei Letzteres für den asymmetrischen Teil der Verschlüsselung zuständig ist. Dieser Algorithmus wird nur für einen Teil des Verschlüsselungsvorgangs eingesetzt, weil die Bearbeitung der Nachricht andernfalls sehr viel Zeit in Anspruch nehmen würde. IDEA und RSA sind die Standardverfahren, die beiden anderen Algorithmen werden eingesetzt, um patentrechtlichen Problemen aus dem Weg zu gehen.

Vor der Verschlüsselung werden die Texte mit einem Pkzip ähnlichen Verfahren komprimiert, zum einen um die Dateigröße herabzusetzen, zum anderen um erkennbare Textmuster, die Ansatzpunkte für Entschlüsselungsversuche bieten könnten, zu

eliminieren.

Dann erzeugt das Programm mit Hilfe eines Zufallszahlengenerators einen temporären symmetrischen Session Key, mit dem die Nachricht verschlüsselt wird. Der Session Key selbst wird mit dem Public Key nach dem asymmetrischen Verfahren kodiert und der Nachricht hinzugefügt.

Um eine gesendete Botschaft elektronisch zu signieren, erzeugt PGP aus der kompletten Nachricht eine 128-Bit-Prüfsumme nach dem Message-Digest-5-Verfahren (RFC 1321), die mit dem privaten Schlüssel kodiert und an die Nachricht angehängt wird. Manipuliert jemand den Inhalt oder tritt ein Übertragungsfehler auf, stimmt die Prüfsumme nicht mehr. Durch dieses Verfahren lässt sich nicht nur die Vertraulichkeit des Inhalts, sondern auch dessen Authentizität garantieren.

Zum Abschluss wird die komplette Nachricht noch nach dem Radix-64-Verfahren in das 7-Bit-ASCII-Format umgewandelt, welches mit dem SMTP als gewöhnliche E-Mail übertragen werden kann.

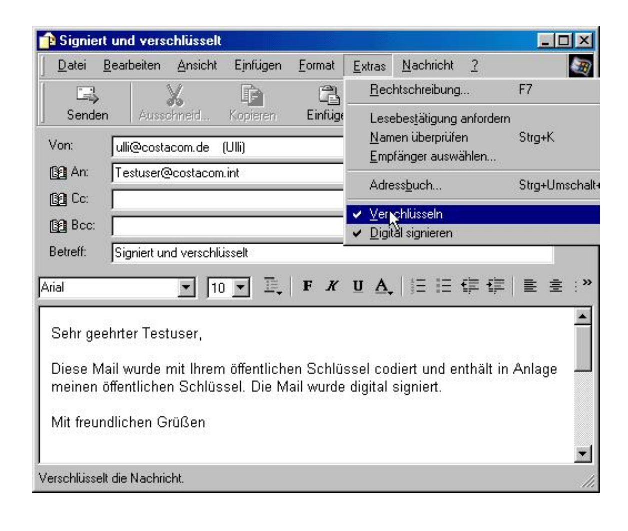
Der Empfänger entschlüsselt zunächst mit dem eigenen asymmetrischen Private Key den temporären Session Key und mit diesem wiederum die eigentliche Nachricht. Im Prinzip handelt es sich bei PGP deshalb nicht um ein reines Public-/Private-Key-Verfahren: Die Nachricht selbst wird nach der konventionellen Methode mit dem gleichen (Session-)Schlüssel kodiert und dekodiert. Die Public-/Private-Key-Verschlüsselung dient nur zum sicheren Übertragen des symmetrischen Schlüssels. Diese kombinierte Methode (Hybrid-Kryptografie) ist auch als *Digitaler Briefumschlag* bekannt.

› Client-Fähigkeiten: Microsoft

Outlook und Outlook Express unterstützen von Haus aus S/MIME, eine auf einem asymmetrischen Verschlüsselungsverfahren basierende MIME-Erweiterung. Um verschlüsselte Nachrichten senden und empfangen zu können, müssen Sie zunächst ein Zertifikat erwerben, welches Sie bei den Empfängern als rechtmäßiger Absender ausweist. Diese Hürde hat bislang verhindert, dass S/MIME eine Akzeptanz wie etwa PGP erfährt. Der Vorteil dieses Systems besteht darin, dass durch die gesicherte Identifizierung des Benutzers neben vertraulichen E-Mail-Informationen auch geschäftliche Transaktionen zuverlässig per E-Mail ausgeführt werden können.

Die dreiteiligen digitalen IDs für S/MIME bestehen aus einem öffentlichen und einem privaten Schlüssel sowie aus einer digitalen Signatur. Der öffentliche Schlüssel dient dem Absender zum Verschlüsseln der Nachricht, anhand der Signatur kann der Absender zweifelsfrei identifiziert werden. Mit dem zugehörigen privaten Schlüssel hat der Empfänger die Möglichkeit, die verschlüsselte Nachricht zu öffnen.

Outlook (Express) unterstützt den komfortablen Einsatz der Signaturen und Schlüssel, indem sich diese in das Adressbuch einbinden lassen. Beim Verfassen der Mail wird die gewünschte Option (Signieren und/oder Verschlüsseln) bei Outlook Express einfach über das Menü*Extras* aktiviert.



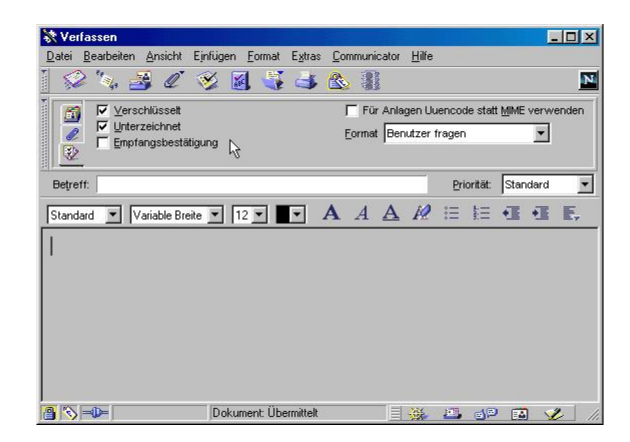
Komfortabel: Beim Erstellen einer Outlook-Express-Mail lassen sich Signatur und Verschlüsselung per Mausklick aktivieren.

Sobald Sie mit einem anderen Benutzer digitale Zertifikate ausgetauscht haben, können Sie von diesem verschlüsselte Mails wie gewöhnliche Mails lesen.

Digitale Zertifikate werden von mehreren Anbietern ausgegeben. Bekannt sind etwa VeriSign (http://www.verisign.com/) und GlobalSign (http://www.globalsign.com/) . Weitere Informationen erhalten Sie auf der Microsoft-Zertifizierungs-Webseite (http://www.microsoft.com/windows/ie_intl/de/features/certpage.htm) .

› Client-Fähigkeiten: Netscape

Auch der Netscape Messenger unterstützt Zertifikate und das Senden und Empfangen von mit S/MIME verschlüsselten Mails. Durch Anklicken des Schlosses in der Statuszeile erscheint das Fenster, in dem Sie die Sicherheitseinstellungen konfigurieren können. Je nach Zertifikat stehen dabei mehrere Optionen bis hin zur Wahl der Verschlüsselungsstärke zur Verfügung. Beim Erstellen einer Mail mit dem Netscape Messenger gelangen Sie über *Ansicht/Optionen* zu einem Menü, in dem Sie das Signieren und Verschlüsseln der Nachricht aktivieren können.



Integriert: Der Netscape Messenger bietet ebenfalls die Möglichkeit, S/MIME-Mails zu versenden.

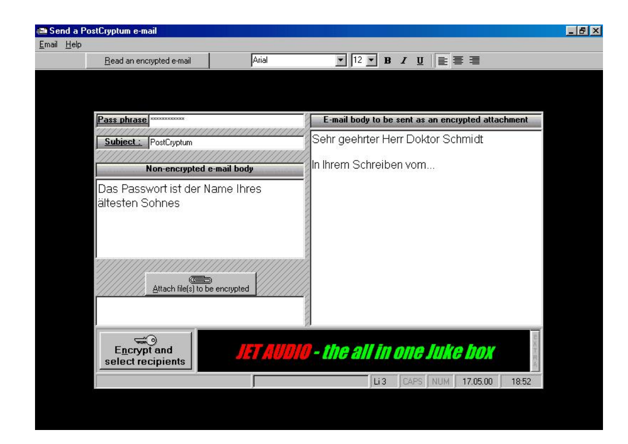
Auch für Netscape (http://www.netscape.com/) ist VeriSign (http://www.verisign.com) ein Partner erster Wahl. Ein persönliches Zertifikat für Netscape Messenger und Microsoft Outlook (Express) kann dort für 15 Dollar pro Jahr erworben werden. Die Verschlüsselungsstärke beträgt zwischen 512 und 1024 Bit. Bei der Beantragung ist zu beachten, dass das Zertifikat browsergebunden ist. Man kann also mit einem Zertifikat nicht gleichzeitig mit Messenger und Outlook Mails signieren.

› Andere Clients und Add-ons

Neben Netscape Messenger und Microsoft Outlook zählt besonders Eudora (http://www.eudora.com/) zu den populären E-Mail-Clients. Das Programm bietet von Haus aus keine Sicherheitsfunktionen, arbeitet aber reibungslos mit Pretty Good Privacy (PGP) zusammen. PGP stellt für die Verschlüsselung von E-Mails mit Eudora ein spezielles Plug-in zur Verfügung, mit dem problemlos die Erzeugung verschlüsselter Mails gelingt.

Eine Reihe weiterer Tools hilft dabei, E-Mails vor neugierigen Augen zu schützen. Sie verfügen allerdings oft nicht über die Verschlüsselungstiefe der professionellen Lösungen.

PostCryptum (http://www.postcryptum.com) arbeitet parallel zu Microsoft Outlook (Express) oder Exchange und erlaubt die partielle Verschlüsselung von Nachrichten. Dabei werden je eine unverschlüsselte und eine verschlüsselte Mail parallel gesendet. Somit ist es möglich, dem Empfänger im unverschlüsselten Bereich einen Hinweis auf das nötige Passwort zu geben. Das Programm ist für den nichtkommerziellen Gebrauch Freeware.

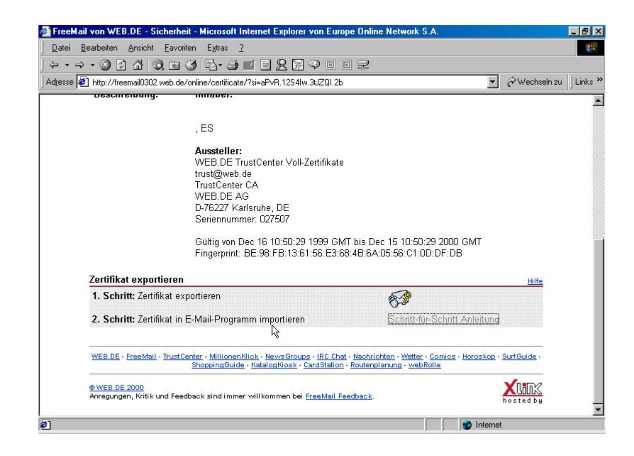


Tipp inklusive: PostCryptum erlaubt die partielle Verschlüsselung von Nachrichten, so dass im unverschlüsselten Bereich Hinweise auf das Passwort gegeben werden können.

A-Lock (http://www.pc-encrypt.com) arbeitet mit allen gängigen E-Mail-Programmen zusammen. Durch Anklicken des A-Lock-Icons in der Taskleiste werden die Inhalte des Mailfensters automatisch ent- beziehungsweise verschlüsselt. Die Verschlüsselungstiefe des symmetrischen Algorithmus beträgt bei der internationalen Version 56 Bit, was etwa einer asymmetrischen Verschlüsselung von 900 Bit entspricht. Das Programm ist Shareware, die Registrierung kostet 15 Dollar.

› Web-Mailprovider mit E-Mail-Verschlüsselung

Webbasierte E-Mail-Dienste (http://www.tecchannel.de/internet/87/index.html) gibt es wie Sand am Meer. Allerdings bieten nur wenige Sicherheitsfunktionen, die über den allgemeinen Standard hinausgehen. Von den deutschsprachigen Anbietern ist FreeMail (http://freemail.web.de/) von WEB.DE derzeit der einzige, der digitale Verschlüsselung erlaubt. Die Verschlüsselungsstärke kann in mehreren Stufen bis maximal 168 Bit gewählt werden. Das Web-Interface ist jedoch nicht hundertprozentig sicher, da Ihre Nachrichten auf dem Weg zum und vom Web-Postfach unverschlüsselt sind.



Kostenlos: FreeMail von WEB.DE bietet kostenlose digitale Zertifikate, die Sie auch aus E-Mail-Clients nutzen können.

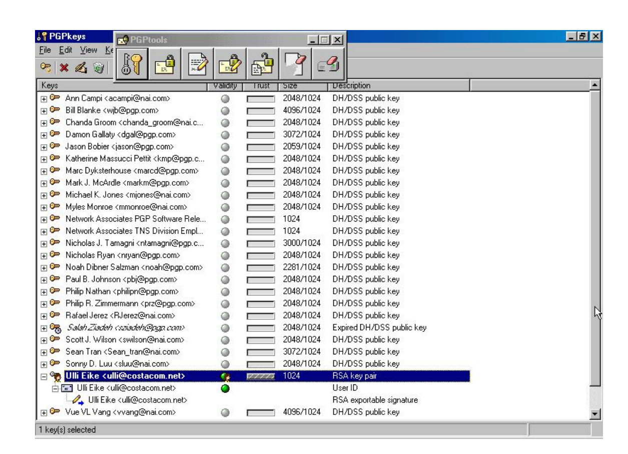
Da man den FreeMail-Service auch mit herkömmlichen E-Mail-Clients und POP/SMTP-Zugang nutzen kann, ist dies ein kostengünstiger Weg, die Sicherheit eines digitalen Zertifikats für die persönliche Korrespondenz zu nutzen. Allerdings ist dieses Zertifikat an die FreeMail-Adresse gebunden und somit nur begrenzt für den professionellen Auftritt nutzbar. Für die Nutzung aus dem E-Mail-Client muss das Zertifikat zunächst exportiert und danach in den gewünschten Client eingebunden werden. Zusätzlich ist der Download der übergeordneten Zertifikate von WEB.DE nötig, um die Zertifizierung zu ermöglichen.

Ein internationales Angebot, welches höchst mögliche Privatsphäre verspricht, kommt von PrivacyX (http://www.privacyx.com) . Neben einem kostenlosen digitalen Zertifikat bietet der Service auch eine völlig anonyme Benutzerregistrierung. Allerdings zeigte sich in der

Praxis, dass mit und an PrivacyX gesendete Mails teilweise mit Verzögerungen bis zu einem Tag beim Empfänger eintrafen. Für einen professionellen Einsatz bei zeitkritischen Anwendungen ist dieses System deshalb nicht zu empfehlen.

› Externe Programme: PGP

Pretty Good Privacy (PGP) hat sich als Standard unter den Stand-alone-Verschlüsselungsprogrammen etabliert und wird weltweit von mehr als 6 Millionen Benutzern eingesetzt.



Standard: Pretty Good Privacy ist der weltweite De-facto-Standard für E-Mail-Verschlüsselung.

Aufgrund der ehemaligen Exportbeschränkungen der US-Regierung und patentrechtlicher Bestimmungen haben sich zwei weit gehend identische Versionen entwickelt, PGP und PGPi, wobei das *i* für *international* steht. Für den nicht kommerziellen Gebrauch sind Freeware-Versionen erhältlich. Die zentrale Anlaufstelle für Informationen ist die PGP-International-Freeware-Website (http://www.pgpi.org/) . Die aktuelle Versionsnummer ist 6.5.3, die nun für alle Benutzer starke Verschlüsselung bietet. PGP 6.5.1i ist die letzte Version, die auch im Quellcode verfügbar ist. Die Leistungsfähigkeit der Versionen unterscheidet sich für den Anwender nicht, im Prinzip basiert die internationale Version auf dem gleichen Code. Dieser musste allerdings als gedrucktes Buch aus den USA exportiert und eingescannt werden, der Export im digitalen Format war verboten.

PGP enthält Plug-ins für viele E-Mail-Clients, so dass die nahtlose Integration in den Arbeitsablauf möglich ist. Unterstützt werden unter anderem Outlook, Outlook Express, Eudora, Lotus Notes und Pegasus Mail. Da es kein offenes API für bisherige Netscape-Versionen gab, müssen sich Messenger-Anwender mit der Verschlüsselung über die Zwischenablage begnügen.

Die Verschlüsselungsstärke von PGP ist mit maximal 2048 Bit sehr hoch. Eine 1024-Bit-Verschlüsselung sollte für herkömmliche Sicherheitsbedürfnisse jedoch ausreichen. Eine ausführliche Dokumentation von PGP findet sich bei FoeBuD. (http://www.foebud.org/pgp/html/pgp.html) . Neben den Freeware-Versionen von PGP(i) existieren Versionen für den kommerziellen Einsatz. Informationen dazu erhält man auf den Websites von PGP (http://www.pgp.com) beziehungsweise PGP International (http://www.pgpinternational.com/) .

› Fazit

Es gibt zahlreiche Möglichkeiten, E-Mails vor den Augen neugieriger Mitleser zu schützen. Entscheidend ist, dass die Sicherheit gewährleistet und das Programm weit verbreitet ist. In dieser Hinsicht hat PGP klar die Nase vorn, 6 Millionen Benutzer sprechen eine deutliche Sprache. Die kostenlosen Versionen kann jeder Privatanwender nutzen und die Erzeugung eines eigenen Schlüssels ist weder mit übermäßigem Aufwand noch mit besonderen Kosten verbunden. Deshalb dürfte sich dieses System auch langfristig im Markt behaupten. Die Unterstützung der populären E-Mail-Clients und die Möglichkeit, das Programm unter mehreren Betriebssystemen einzusetzen, machen

es für nahezu jeden Anwender attraktiv.

Die in E-Mail-Clients integrierten S/MIME-Lösungen sind ebenfalls bequem und sicher. Der Benutzer kann jedoch noch nicht damit rechnen, dass seine Kommunikationspartner ebenfalls S/MIME nutzen.

Wenn man einzelne Mails verschlüsseln will, sind webbasierte E-Mail-Clients eine brauchbare Alternative. Sie bieten jedoch weder den Komfort noch die Sicherheit, die im täglichen Einsatz ausschlaggebend sein werden. (tri)

› Weitere Themen zu diesem Artikel:

Lauschangriff im Firmennetz (http://www.tecchannel.de/internet/288/index.html)
Kostenlose E-Mail-Dienste (http://www.tecchannel.de/internet/87/index.html)

Webdienste und Sicherheit

› Das Thema Webdienste und Sicherheit wird im Jahr 2003 heiß diskutiert. Auch wenn Microsoft mit der ".Net-Initiative" und Sun mit "Sun-One" auf eine schnelle Markteinführung hoffen, sollte der Einsatz in Unternehmen wohl überlegt erfolgen.

› VON RAY WAGNER UND FRANK KLINKENBERG

Webdienste gelten allgemein als nächste Stufe der Applikationsintegration und Zugang zu neuen Geschäftsmodellen sowie als beispiellose Vernetzungsmöglichkeit für Unternehmen. Sicherheitsbedenken und die Komplexität der Sicherheitsmechanismen für Webdienste werden jedoch dazu beitragen, dass deren Angebot in naher Zukunft überwiegend einfach und zurückhaltend ausfällt.

Das Marktforschungsinstitut Gartner (http://www.gartner.com) empfiehlt Unternehmen, sich vor einem großflächigen Einsatz zunächst intensiv mit der zu Grunde liegenden Technologie vertraut zu machen. Best-Practice-Modelle raten Unternehmen für 2003 zu einer vorsichtigen Herangehensweise beim externen Einsatz von Webdiensten. Bevor sie das High-Value-Segment bedienen, sollten Firmen ihr Know-how weiterhin durch interne Ausbildung und Entwicklungsanstrengungen ausbauen und sich mit Webdienste-Standards und -technologien stärker vertraut machen. Durch diesen Ansatz kann sich der Markt für Webdienste-Sicherheits- und -Managementlösungen entwickeln, während sich Standards etablieren.

Dies hat zur Folge, dass die meisten Unternehmen ihre Webdienste-Initiativen 2003 zurückstellen oder zunächst durch interne Applikationsintegration Erfahrung mit der Technologie sammeln. Diese Firmen werden Webdienste erst 2004 oder später einsetzen, wenn Standards und Produkte ausgereift und Unternehmen im Umgang mit der Technologie vertrauter sind. Außerdem bleiben, obwohl die größeren Anbieter gute Fortschritte bei Initiativen für Webdienste-Sicherheitsstandards machen, wichtige Trust-Fragen unbeantwortet und größtenteils unberücksichtigt. Dies wird die Einführung ebenfalls verlangsamen.

› Basiskomponenten für sichere Webdienste

Bis jetzt zeigen sich die großen Anbieter und Wettbewerber auf dem Markt für Webdienste bei der Entwicklung von Sicherheitsstandards kooperationsbereit. Denn sie erkennen, dass Webdienste keine breite Akzeptanz erlangen werden, ohne geeignete Mechanismen, die die Geheimhaltung, Vertraulichkeit und Integrität von Transaktionen gewährleisten. Es wird jedoch erwartet, dass die Auseinandersetzungen um Standards deutlich zunehmen, da die Aufmerksamkeit der Industrie sich dem Federated-Identity-Konzept (etwa der Liberty Alliance und Microsoft Passport) und komplexeren Erweiterungen der Web-Services-Security-Spezifikation zuwendet. Trotzdem werden die Basiskomponenten für sichere Webdienste verfügbar sein. Dazu zählen:

- › Web Services Description Language zur Integrität
- › Security Assertion Markup Language zur Authentifizierung und Authorisierung
- › Secure Sockets Layer (SSL) zur Absicherung von Übertragungskanälen
- › XML-Verschlüsselung zur granularen Steuerung der Vertraulichkeit
- › Digitale XML-Signatur zur granularen Feststellung der Verbindlichkeit

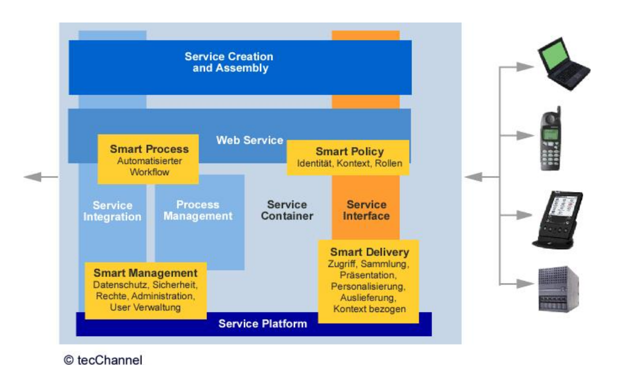
Einige weitere Schlüsselstandards erreichen wahrscheinlich in naher Zukunft Release-Status, darunter:

- › Web Services Security (einschließlich XML-Verschlüsselung und Digitale XML-Signatur)
- › XML Key Management Specification zur Schlüsselverwaltung
- › Extensible Access Control Markup Language zur Authorisierung

› Entwicklungen für komplexe Dienste

Komplexe, hochwertige Webdienstangebote werden indes die Ausnahme sein. Die brisanten Trust-Fragen, die der PKI-Industrie zugesetzt haben, verstellen die klare Sicht auf die Vorzüge von Webdiensten. Unternehmen, die die 1999 getätigten Ausgaben für den Einsatz der PKI nicht rechtfertigen konnten, werden wohl auch nicht in der Lage sein, vergleichbare Kosten für die Sicherheit komplexer Webdienstangebote 2003 zu erklären, besonders unter den momentan herrschenden Marktbedingungen.

Kurzfristig werden Unternehmen Webdienste daher nur intern einsetzen oder abgespeckte externe Angebote in Betracht ziehen (vergleichbar mit den frühen Webauftritten von Firmen, die ihre Prospekte einfach 1:1 ins Internet übertragen hatten). Höherwertige Transaktionen, die auf Verbindungen mit bekannten Geschäftspartnern basieren, dürften für die meisten Unternehmen 2003 kaum in Betracht kommen.



Arbeitsteilung: So integrieren sich intelligente Webdienste in eine bestehende Umgebung.

Bis 2004 werden Web Services Security und XML Key Management Specification eine relativ komplette Basis für Sicherheitsstandards schaffen. Wenn diese grundlegenden Sicherheitsstandards definiert sind, kommen auch entsprechende Produkte für Webdienste auf den Markt. Größere Anbieter treten in den Markt ein oder kaufen kleinere Start-ups auf. Firmen, die planen, Webdienste auch extern anzubieten, werden daher erst 2004 aus einer Palette von vergleichsweise ausgereiften Sicherheitsprodukten auswählen können.

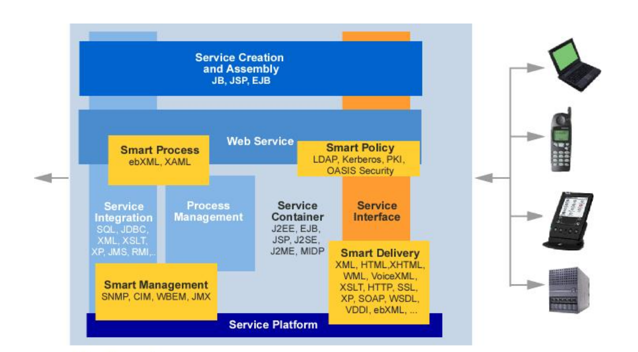
Unternehmen werden bis Ende 2003 aber dennoch in der Lage sein, sorgfältig geplante und entworfene Webdienste mit Perimeter-Mechanismen (statt integrierten Mechanismen) sicher anzubieten. Firmen und Abteilungen, die sich auf die Architektur von Webdiensten konzentrieren, finden eine gute Ausgangslage vor, um im Jahr 2003 die Basis für Architektur und Entwicklung zu schaffen.

› Interne Entwickler als Motor für Webdienste

Webdienste sind eine äußerst attraktive Möglichkeit für Entwickler, die sich mit Problemen der Applikationsintegration und Kommunikation beschäftigen. Sie sind auch mächtige Werkzeuge, mit denen sich neue Geschäftsmodelle entwickeln lassen, die die innerbetriebliche Koordination verbessern.

Wie bei jedem mächtigen und vielseitigen Tool (etwa dem Internet oder PCs), werden Entwickler die Möglichkeiten dieser Technologie erkennen und Webdienste rasch dazu benutzen, um taktische Probleme zu lösen und Strategien zu implementieren - oft jedoch, ohne sich ausreichend um Sicherheits- oder Effizienzfragen zu kümmern. Hinzu kommt, dass der Großteil neuer Unternehmens-Software wahrscheinlich mit Schnittstellen für Webdienste ausgestattet ist, so dass das IT-Management und die Security-Abteilung

Mühe haben werden, die Nutzung von Webdiensten in ihren Organisationen zu steuern.



Ohne Standards geht nichts: Um Diensteanbieter, -benutzer und -entwickler unter einen Hut zu bringen, müssen sich alle auf gemeinsame Standards einigen.

Unternehmen, die sich mit den Möglichkeiten von Webdiensten beschäftigen und deren Einsatz konservativ planen, dürften entdecken, dass interne Abteilungen, die praktische Lösungen für bestimmte Probleme des operativen Betriebs wollen, diese Dienste bereits einsetzen. Viele dieser "Quick-and-Dirty-Lösungen" werden jedoch gravierende Sicherheitslücken aufweisen oder Sicherheitsbedenken ignorieren. Man kann davon ausgehen, dass bis zum zweiten Halbjahr 2004 etwa 40 Prozent der Global-2000-Unternehmen ungenehmigte, undokumentierte und nicht überwachte externe Webdienste-Verbindungen unterhalten.

Jedes Unternehmen, das den Einsatz von Webdiensten für die Applikationsintegration und neue Anwendungen plant, sollte sich daher mit dieser Technologie auseinander setzen und Richtlinien zur Überwachung und Kontrolle der internen und externen Nutzung erstellen.

› Gefahren durch Webdienste

In dem Maße wie Unternehmen sich mit einer Umgebung konfrontiert sehen, in der Webdienste kaum noch wegzudenken sind, werden sie erkennen, dass externe Übertragungen über HTTP oder auch HTTPS potenziell gefährlich sind. Gartner etwa sagt voraus, dass Webdienste 70 Prozent der Angriffspfade wieder öffnen, die in den letzten zehn Jahren durch Firewalls geschlossen wurden. Denn Webdienste können herkömmliche Schutzmaßnahmen in Unternehmen umgehen, beliebige Schadfunktionen enthalten und mit fast jeder Ressource im Unternehmen interagieren. Zum Unternehmensschutz wird es ein gewisses Maß an Kontrolle der Übertragungen auf Applikationsebene geben müssen.

In Unternehmen kommt hinzu, dass der HTTP- und HTTPS-Traffic überdurchschnittlich zunimmt, wenn mehr Applikationen über XML und SOAP kommunizieren. Mit dem Release von Microsofts .NET-Server und kommenden Windows- und Office-Versionen, die Webdienste verstärkt nutzen, steigt dieser Trend. Bekannte Fehler in Protokollen von Webdiensten und darauf basierenden Produkten bedingen, dass sich Systemadministratoren zunehmend mit Management- und Überwachungssystemen, einschließlich Sicherheitssystemen, befassen müssen. Bis 2005 werden Best-Practice-Konzepte daher fordern, dass nicht registrierter HTTP- und HTTPS-Traffic am Grenzbereich zum Unternehmen kontrolliert wird. Dies bedingt die Möglichkeit zur Prüfung auf Applikationsebene - insbesondere XML, SOAP und Webdienste - mit Technologien der Perimetersicherheit.

Die meisten Sicherheitsmechanismen für Webdienste lassen sich Perimeter-basiert realisieren. Daher sollten Unternehmen Tools wie Sicherheits-Gateways, SSL-Konzentratoren und -Beschleuniger sowie SOAP/XML-Prüf-Hardware, die bei Leitungsgeschwindigkeit arbeitet, erproben. Durch eine strategische Planung können Unternehmen die Architekturklassen für Webdienste bestimmen, die für ihre Bedürfnisse am besten geeignet sind.

› Fazit: Keep it simple

Einfachheit wird zunächst die vorherrschende Strategie für Webdienste sein. Denn die Technologie von Webdiensten und deren Sicherheitsmechanismen befinden sich noch im Anfangsstadium. Die Notwendigkeit für den Business-Einsatz von Webdiensten liegt zwar auf der Hand, doch die meisten Unternehmen werden diese zunächst nur zögernd einsetzen. Denn bei missionskritischen Anwendungen will man von neuen Technologien unabhängig sein, bis diese als verlässlich gelten. Außerdem erfordern komplexe Webdienste mit mehreren Teilnehmern (wie derzeit vorgeschlagen) erhebliche Ressourcen für Sicherheitsmaßnahmen, inklusive PKI.

Die meisten Firmen werden daher in naher Zukunft einfache Webdienste im Low-Value-Segment erwägen und dabei auf der Suche nach einfachen und kostengünstigen Sicherheitsmechanismen sein. Die meisten Webdienste-Angebote - selbst wenn sie als einfach gelten - werden es erfordern, dass der Service Provider auch für die Verbindungsbereitstellung Endkunden-Support bietet.

Bis 2005 werden Kosten, Komplexität und mangelnde Erfahrung mit den erforderlichen Sicherheitsmechanismen 80 Prozent der externen Webdienst-Angebote auf einfache Punkt-zu-Punkt-Architekturen zurückführen, die nur durch SSL-Serverzertifikate gesichert sind.

Empfehlung für 2003: Unternehmen, die bis jetzt noch keine PKI eingeführt haben, sollten dies auch in naher Zukunft nicht tun. Es sei denn, sie setzen dringend benötigte Applikationen ein, die Key-Management erfordern. Betriebe, die Sicherheitsplattformen für Webdienste kaufen, sollten darauf bestehen, dass sie die volle Leistung von Standard-SSL-Serverzertifikaten nutzen können - nicht nur zur Kanalverschlüsselung, sondern auch zur Zwei-Wege-Authentifizierung und digitalen Signatur von Transaktionen.

Firmen, die überlegen, Webdienste-Technologien auf breiter Front zu nutzen, sollten sich darauf einrichten, in Maßnahmen zur SSL-Beschleunigung und -Konzentration zu investieren. Generell empfehlen wir Unternehmen, die Webdienste-Technologie vorsichtig und überlegt einzuführen. (Thomas Rieske/fkh)

Anmerkung: Dieser Beitrag erschien im Original (http://www.csoonline.com/analyst/report709.html) *in unserer US-Schwesterpublikation CSO. Es handelt sich dabei um die Analyse einer Studie von Gartner zum Thema "Webservices und Sicherheit im Jahr 2003".*

› Weitere Themen zu diesem Artikel:

Windows .NET Server RC1 (http://www.tecchannel.de/betriebssysteme/993/index.html)
Microsoft .NET versus Sun ONE (http://www.tecchannel.de/betriebssysteme/616/index.html)
JavaOne: Gegenpol zu Microsoft .NET (http://www.tecchannel.de/internet/899/index.html)
Microsofts .NET als Open Source? (http://www.tecchannel.de/betriebssysteme/748/index.html)
Firewall-Grundlagen (http://www.tecchannel.de/internet/682/index.html)
Kryptographie-Grundlagen (http://www.tecchannel.de/internet/416/index.html)
Praxis der digitalen Signatur (http://www.tecchannel.de/internet/909/index.html)

Dem Surfer auf der Spur

› Schwer vorstellbar, dass jemand in der Lage sein sollte, Spuren im Internet zu verfolgen. Aber Privatsphäre im Netz ist eine Illusion, Anonymität für den Surfer gibt es nicht. Es sei denn, man ergreift einige grundlegende Abwehrmaßnahmen.

› VON ULLI EIKE UND RA RAINER WERTENAUER

Anonyme Anrufer haben schlechte Karten, wenn die Nummer des eigenen Anschlusses im Display des Angerufenen erscheint. Und die detaillierte Telefonabrechnung mit gewählter Nummer, Gesprächsdatum, -uhrzeit und -dauer macht auch unbekümmerten Naturen klar, dass private Daten keineswegs geheim sind.

Was beim Telefon revolutionär erschien, gehört im Internet zur Grundausstattung. Die TCP/IP-Technologie basiert darauf, dass eine Verbindung zwischen zwei definierten IP-Adressen aufgebaut wird. Statt einer komplizierten Fangschaltung reicht ein einfacher "Ping", um die digitale Adresse der Gegenstelle zu ermitteln. Schlimmer noch: Beim Betreten einer Website liefert der eigene Browser bereitwillig eine Reihe von Informationen. Diese reichen von belanglosen technischen Spezifikationen bis hin zu intimen Daten wie der zuletzt besuchten Website und eventuell der eigenen E-Mail-Adresse.

Für den Betreiber kommerzieller Websites ist dies eine wahre Freude: Schließlich kann er anhand der statistischen Daten sein Angebot besser auf seine Besucher ausrichten. Das ist jedoch nicht alles. Mit Hilfe von Formularen, die der Besucher etwa zum Download von Software, der Teilnahme an einem Preisausschreiben oder bei einer Bestellung ausfüllen muss, erstellen Firmen detaillierte Profile. Durch den Einsatz von Cookies ist es problemlos möglich, jedem Besucher sein eignes Profil zuzuordnen. Eine Website mit 100.000 Hits pro Tag erkennt die Besucher leichter und schneller wieder als der Bäcker um die Ecke seine Kunden, die morgens Ihre Brötchen holen. Und wer über Links auf andere Sites wechselt, hinterlässt eine deutliche Spur. Anders als beim Bäcker sieht man ihm an, ob er gerade aus einem Sexshop kommt.

Die Datensammlungen werfen nicht nur rechtliche Fragen auf, was Website-Betreiber mit den Daten alles anstellen dürfen. Details dazu lesen Sie am Ende dieses Artikels. Problematisch ist ebenso das Eindringen in die Privatsphäre, das größtenteils unbemerkt geschieht. Wie es Michael Swaine in seinem tecVision-Beitrag (http://www.tecchannel.de/tecvision/191/index.html) geschildert hat, steht der gläserne Surfer längst nicht mehr am Horizont, sondern direkt vor unserer Nase.

› Sicher unsicher im Web

Vielleicht zucken Sie als vorsichtiger Surfer mit den Achseln und verweisen darauf, dass Sie in Formularen ohnedies immer einen falschen Namen angeben. Wahrscheinlich besitzen Sie fantasievolle E-Mail-Identitäten bei diversen Webmail-Diensten. Sicher, Ihre Identifikation wird damit erschwert, aber Ihr richtiger Name ist für die meisten Zwecke sowieso nicht wichtig. Interessant ist vor allem, was Sie kaufen und wofür Sie sich interessieren. Selbst wenn Sie in Formularen Ihr Jahreseinkommen verschweigen: Der Erwerb der Bang&Olufsen-Anlage über das Internet und Ihr permanentes Interesse an den Ausstattungsdetails der S-Klasse enttarnen Sie als Mitglied der kaufkräftigen Zielgruppe. Diese gilt es mit optimierter Werbung zu erreichen, egal wie Sie sich nennen.

Bislang ist die Welt noch in Ordnung. Sie besitzen genug Souveränität, um Ihre Kaufentscheidungen mit kühlem Kopf zu treffen. Was aber, wenn Ihre Daten einmal in falsche Hände geraten? Dass Websites unsicher sind, wird nahezu täglich bewiesen: Zwei Datenbank-Hacks und die anschließende Veröffentlichung Tausender Kreditkartendaten allein im Januar sprechen eine deutliche Sprache. Ihre Anschrift,

Kreditkartennummer, Bankverbindung und vielleicht noch die Internet-Reservierung des zweiwöchigen Familienurlaubs in der Karibik mit genauen Reiseterminen können in den falschen Händen für eine Menge Ärger sorgen. Einbrecher könnten sich bedanken, wenn Sie sich in Diskussionsforen rege zum geplanten Urlaub äußern und gleichzeitig über eine der beliebten Visitenkarten hans@müller.de verfügen. Eine einfache Whois-Anfrage beim DENIC (http://www.denic.de/) gibt Auskunft über die Adresse, unter der die Domain registriert ist.



RIPE
homepage | what's new | whois db | search | site map | f.a.q.

tecchannel.de

```
% Rights restricted by copyright. See http://www.ripe.net/ripencc/pub-services/db/copyright.html

domain:   tecchannel.de
descr:    IDG Magazine Verlag GmbH
descr:    Brabanter Strasse 4
descr:    D-80805 Muenchen
descr:    GERMANY
admin-c:  JH4598-RIPE
tech-c:   COLT2-RIPE
zone-c:   COLT2-RIPE
nserver:  ns0.de.colt.net
nserver:  ns1.de.colt.net
nserver:  ns2.de.colt.net
mnt-by:   DE-DOM
changed:  hostmaster@denic.de 19991130
source:   RIPE

role:     COLT Germany Hostmaster
address:  COLT TELECOM GmbH
address:  Gervinusstrasse 18-22
address:  D-60322 Frankfurt
phone:    +49 69 95958 0
fax-no:   +49 69 95958 250
e-mail:   hostmaster@de.colt.net
trouble:  Call 0130 182223 (from Germany)
trouble:  or call +49 69 95958 550
admin-c:  FH3800-RIPE
tech-c:   RW11-RIPE
tech-c:   MB15202-RIPE
nic-hdl:  COLT2-RIPE
mnt-by:   DE-COLT-MNT
changed:  bernward@de.colt.net 19981229
changed:  mbind@de.colt.net 20000201
source:   RIPE

person:   Joachim Herbert
address:  IDG Magazine Verlag GmbH
address:  Leopoldstrasse 252b
address:  D-80807 Muenchen
address:  GERMANY
phone:    +49 89 36086121
fax-no:   +49 89 36086267
e-mail:   jherbert@pcwelt.de
nic-hdl:  JH4598-RIPE
changed:  auto-direct@denic.de 19990729
changed:  auto-direct@denic.de 20000121
source:   RIPE
```

Blid 1: Eine einfache RIPE- oder DENIC-Anfrage erlaubt jedermann Zugriff auf Ihre Adresse und Telefonnummer.

Zum Thema E-Mail warnende Worte zu verlieren, ist wohl überflüssig. Der Postmaster Ihres Mailservers kann diese genauso lesen wie jeder, der irgendwann mal Zugang zum Rechner des Empfängers bekommt. Dass alle dazwischen liegenden Stationen ebenfalls dazu die Gelegenheit haben, macht die Sache nicht mehr viel schlimmer.

Auf den folgenden Seiten lesen Sie, was im Einzelnen mit Ihren Informationen geschieht und wie Sie sich vor den schlimmsten Verletzungen Ihrer Privatsphäre schützen können.

› Was Websites von Ihnen wissen

Bevor Sie weiterlesen, klicken Sie bitte auf diesen Link (http://privacy.net/anonymizer/) . Sie sehen eine beträchtliche Datensammlung, die automatisch über Sie zusammengetragen wurde.

Da ist zunächst Ihre aktuelle IP, die der Server, mit dem Sie kommunizieren, zumindest temporär speichert. Das ist kein böser Wille, sondern zwingende Notwendigkeit, um Ihnen die gewünschten Daten senden zu können. Jede kommerzielle Site verfügt über ein Logfile, in dem sie alle IP-Adressen speichert.

Sollten Sie eine feste IP besitzen, sind Sie (beziehungsweise Ihr Computer) eindeutig identifizierbar. Mittels der RIPE-Whois-Abfrage (http://www.ripe.net/cgi-bin/whois) lässt sich, im Gegensatz zum DENIC, zusätzlich der Besitzer einer IP ermitteln.

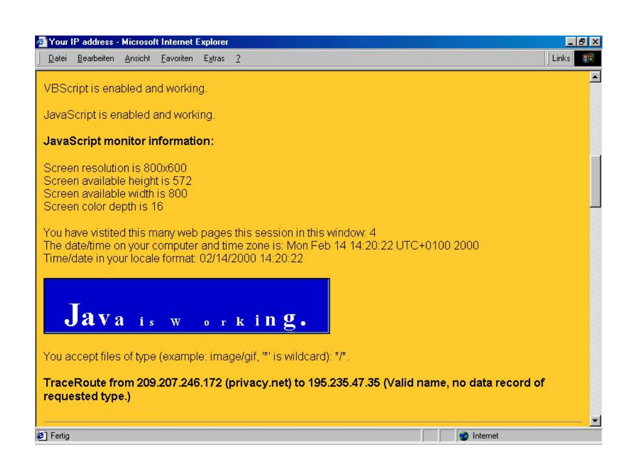


Bild 2: Der Anonymizer zeigt Ihnen beispielhaft, wie viele Informationen Sie beim Surfen ungewollt über sich preisgeben.

Sollte Ihr Provider Ihnen eine feste oder eine dynamische IP zugewiesen haben, ist dazu ein weiterer Schritt nötig: Man muss den Provider (der bei RIPE als der Besitzer der IP gespeichert ist) zur Herausgabe seiner Logdateien bewegen. Dazu ist er beispielsweise verpflichtet, wenn sich auf Grund illegaler Aktivitäten des Surfers der Strafverfolgungsapparat in Bewegung gesetzt hat. Aber schwarze Schafe unter den Betreibern geben die Daten auch so heraus. Sie verfolgen alle Aktivitäten ihrer Nutzer, legen Bewegungsprofile an und verkaufen die Benutzerdaten.

Ihr Browser gibt über den http-Header sowie auf Anfrage weitere Daten preis, die eher statistischen Wert haben. Diese betreffen in erster Linie Ihr Betriebssystem, Ihre Bildschirmdarstellung sowie aktivierte Funktionen. Interessant sind dabei die benutzte Sprache und die Zeitzone, in der Sie sich befinden. Mit hoher Wahrscheinlichkeit lässt sich so ohne besondere IP-Recherchen Ihr Herkunftsland ermitteln.

› Surfgewohnheiten erfasst

Der Browser liefert weitere Informationen, welche die Zahl der von Ihnen in dieser Sitzung besuchten Seiten und die letzte Adresse betreffen. Kommen Sie von AOL und die Zahl der zuvor besuchten Seiten ist "1"? Dann sind Sie mit ziemlicher Sicherheit AOL-Kunde und man zwingt Ihnen die Werbung anderer Provider auf. Besuchen Sie Opel nun schon zum dritten Mal und waren zuvor bei VW, Ford und Toyota? Aha, Sie planen demnächst ein Auto zu kaufen.

Der jeweilige Anbieter weiß ganz genau, wofür Sie sich interessieren. Ihre digitale Identität lässt sich in einem Cookie auf Ihrem Computer speichern und beim nächsten Besuch automatisch mit Ihrem Profil beim Anbieter verknüpfen. Zusätzlich zu den erwähnten Daten hat er die Logfiles seines Servers zur Hand. Diese informieren ihn genauestens, welche Seiten Sie sich bei ihm wie lange angesehen haben und wohin Sie schließlich weitergezogen sind. Einige Statistik-Tools geben zudem Auskunft darüber, ob Sie eine Suchmaschine hergeführt hat und welche Suchbegriffe(!) Sie dort eingegeben haben.

Last 20 Referrers from Usenet	Unique Visitors
05 Dec, Fri, 07:17:15	news:01bcad90f34ss32u6@default
05 Dec, Fri, 20:11:36	news:01bcad90jdsfkj88jk65@default
05 Dec, Fri, 21:35:12	news:01bcad90a42f480mj8@default
07 Dec, Sun, 02:26:38	news:01bcad90jdsfkj88jk65@default
07 Dec, Sun, 03:24:17	news:01bcad90ueroihhg5@default
08 Dec, Mon, 12:48:26	news:01bcad90a42f480f1kl@default
08 Dec, Mon, 12:50:11	news:01bcad90a42f480df56@default
08 Dec, Mon, 15:58:10	news:01bcad8fdc2@default
08 Dec, Mon, 23:59:26	news:01bcad90a42f480dc2@default

Last 20 Referrers from Harddisk	Unique Visitors
21 Nov, Fri, 10:30:11	file:///A|/example5.htm
21 Nov, Fri, 13:27:46	file:///C|/USER/start_example.HTM
23 Nov, Sun, 00:06:34	file:///C|/example/Homepage/start.htm
24 Nov, Mon, 11:15:29	file:///a%7C/Link/example.htm
28 Nov, Fri, 02:04:31	file:///C|/Internet/Netscape3/Cache/M0Q7UIOF.HTM
03 Dec, Wed, 07:24:42	file:///I|/Docs/MS/demo/example.htm
15 Dec, Mon, 05:44:15	file:///C|/DIR/SOME/EXAMPLE/DOC1.HTM

Bild 3: Logdateien und Statistiken geben detaillierte Auskunft über Besucher auf einer Website, hier bis hin zu Festplattenpfaden der angeklickten Links.

Weitere Tricks und Kniffe erhöhen das Datenvolumen über Sie. Mittels einer automatisierten http-Anfrage an Ihre IP kann der Betreiber einer Website herausfinden, ob Sie einen Webserver betreiben. Lässt er ein Bild seiner Seite per FTP laden (img src="ftp://..."), gibt ihm Ihr Browser unter Umständen Ihre E-Mail-Adresse preis. Das passiert, wenn Sie Ihre Mail-Verbindung zum anonymen Login auf FTP-Servern in Ihre Browserkonfiguration eingetragen haben. In alten Browsern reicht dazu ein simpler http_from-Request. Der Sitebetreiber kann Sie auch zum Absenden eines Formulars bewegen, um an Ihre E-Mail-Adresse zu gelangen. Das ist manchmal nicht erkennbar, weil sich das Formular hinter einem einfachen Link verbirgt. Allerdings warnt Sie in diesem Fall ein Dialogfenster Ihres Browsers - sofern Sie diese Warnung nicht leichtfertig deaktiviert haben.

› E-Mail: Postgeheimnis ade

Die E-Mail-Adresse des Surfers ist bares Geld wert. Als Anbieter verlockender Produkte muss man nicht warten, bis der Surfer eine bestimmte Site besucht. Hat ein Anbieter erst die E-Mail-Adresse eines potenziellen Kunden, kann er ihn ungefragt mit Werbemails überhäufen. Es ist nicht schwer, an Ihre E-Mail-Adresse zu kommen: Sie müssen sie ja fast täglich preisgeben. Egal ob Sie Software herunterladen, für die Ihnen ein Passwort zugemailt wird, einen Forumsbeitrag verfassen oder einfach nur ein Formular ausfüllen. Durch die Informationen im Header der Nachricht ist es ein Leichtes, den Weg der Mail bis zu dem von Ihnen benutzten Mailserver zurückzuverfolgen. Bedenklich ist, dass die E-Mail durch ihre Struktur womöglich Auskunft über Namen und Provider ihres Besitzers gibt. Noch mehr erfährt man, falls sich der E-Mail-Besitzer in Verzeichnisse wie Bigfoot eingetragen hat.

```
Quelltext
From: SdAmore@tecChannel.de
Received: from SMTP32-FWD by mail.costacom.net
  (SMTP32) id A00000110; Fri,  4 Feb 2000 07:05:32 -0500
Received: from post.webmailer.de [192.67.198.66] by mail.costacom.net with ESMTP
  (SMTPD32-6.00) id A08111CD01BA; Fri, 04 Feb 2000 07:05:21 -0500
Received: from mail.space.net (mail.Space.Net [195.30.0.8])
      by post.webmailer.de (8.9.3/8.8.7) with SMTP id NAA02647
      for <ulli@costacom.de>; Fri, 4 Feb 2000 13:06:28 +0100 (MET)
Received: (qmail 14813 invoked from network); 4 Feb 2000 12:06:28 -0000
Received: from ns01muc.idgcom.de (195.30.185.70)
  by mail.space.net with SMTP; 4 Feb 2000 12:06:28 -0000
To: "Ulli Eike" <ulli@costacom.de>
Subject: Konzept
X-Mailer: Lotus Notes Version 5.0.1 (Intl)  11. August 1999
Message-ID: <0F5FB098CE.D0D5FB68-0NC125687B.00423331@idgcom.de>
Date: Fri, 4 Feb 2000 13:04:27 +0100
X-MIMETrack: MIME-CD by Notes Server on ns01muc/server/idg/de(Release 5.0.2b (Int
 December 1999) at 04.02.2000 13:04:28,
      MIME-CD complete at 04.02.2000 13:04:28,
      Serialize by Router on ns01muc/server/idg/de(Release 5.0.2b (Intl)|16
 December 1999) at 04.02.2000 13:04:29
MIME-Version: 1.0
Content-type: multipart/mixed;
```

Bild 4: Der Kopf einer E-Mail-Nachricht enthält zahlreiche Informationen, die das Aufspüren des Absenders erleichtern.

E-Mails lassen sich weitreichend missbrauchen. Erhalten Sie eine HTML-Mail mit eingebundenem Bild, das vom Server des Absenders abgerufen werden muss, bekommt

dieser gleichzeitig Ihre IP-Adresse frei Haus. Schlimmstenfalls schleicht sich daraufhin der Absender per Telnet in Ihr schlecht gesichertes System ein oder übernimmt mit Tools wie Back Orifice die Kontrolle über Ihren Rechner. Zumindest kann er, wie zuvor beschrieben, per Whois-Abfrage die zugehörige Postadresse ermitteln. Diese Möglichkeiten stehen nicht nur seriösen Internethändlern zur Verfügung, sondern jedem, der einen Beitrag von Ihnen in einem Diskussionsforum liest und Ihnen eine Mail zukommen lassen kann.

Webbasierte Mailservices bieten scheinbar eine Lösung, da die Spur Ihrer Mails zunächst beim Dienstleister versiegt. Im Gegenzug müssen Sie dem Dienstleister viele der Daten geben, die Sie vor anderen verbergen wollen. Er hat nun alle Möglichkeiten, Ihre private Mail auszuspionieren, ein hervorragendes Profil zu erstellen und Sie gezielt mit Werbung zu bombardieren. Sicher sind Ihre Mails und Daten dort nur bis zum nächsten Hack oder bis der Staatsanwalt mit einem Durchsuchungsbefehl vor seiner Tür steht.

› Anonymes Surfen

Ein Proxyserver ist die einzige Methode, die Spuren zu verwischen, die Sie beim Surfen im Internet hinterlassen. Er nimmt Ihre Anforderungen entgegen und leitet die Daten, die er als Antwort erhält, an Sie weiter. Dabei trägt er sich gewissermaßen selbst als Absender ein und besucht quasi stellvertretend für Sie die angeforderte Website. Der Proxyserver deaktiviert Skripts, die beispielsweise Browserinformationen abfragen oder Formulare steuern, und filtert http-Header aus. Keine Information wird unbeabsichtigt weitergeleitet. Je nach Auslastung des Proxys können jedoch erhebliche Verzögerungen eintreten. Ein weiterer Nachteil ist, dass erwünschte Skripts oft nicht mehr funktionieren.

Der bekannteste Vertreter dieser Tarn-Proxys ist Anonymizer (http://www.anonymizer.com/) . Er lässt sich kostenlos (mit Werbeeinblendungen) oder mit erhöhtem Komfort gegen Gebühr nutzen.

Einen Schritt weiter geht der Lucent Personal Web Assistant (http://lpwa.com/) (LPWA), der das Anlegen von Scheinidentitäten erlaubt. Der Surfer bleibt anonym, Websites erkennen ihn jedoch wegen seiner gleich bleibenden (falschen) Identität wieder. Individuelle Einstellungen bleiben so erhalten. Der Nachteil ist, dass Websites Profile für die falsche Identität erstellen - und den Benutzer somit weiter gezielt bewerben können. Der LPWA bietet die zusätzliche Option, E-Mail-Adressen zu verschlüsseln, sodass der Website-Betreiber keine Information über die tatsächliche Adresse bekommt. Ein Mail an die verschlüsselte Adresse leitet der LPWA an die richtige Adresse weiter. Unerwünschte Mails kann der Assistant leicht abblocken, weil er für jede besuchte Site eine neue Adresse generiert.

Etwas bedenklich stimmt das Angebot von Lucent, Benutzernamen und Passwörter sowie Suchanfragen zu speichern. Da Sie sich zur Benutzung registrieren müssen, sind Sie zumindest für Lucent nicht mehr anonym.

› Anonymes Mailen

Eine Verschlüsselungssoftware wie PGP (http://www.pgpi.org/) (Pretty Good Privacy) ist die beste Methode, um Ihre Mails gegen neugierige Blicke zu schützen. Nur der legitime Empfänger kann auf den Inhalt zugreifen, für alle Zwischenstationen ist der Text der Nachricht unlesbar.

Für den anonymen Versand von E-Mails gibt es mehrere Methoden. Sehr sicher sind so genannte Anonyme Remailer, eine Kette von Mailservern, die eine Nachricht so weiterleiten, dass ihr Weg nicht mehr nachvollziehbar ist. Dazu bedienen sie sich mehrerer Verschleierungsmethoden. Unter anderem verzögern sie die Weiterleitung der eintreffenden Mails um einen Zufallswert und ändern die Größe der Datei unterwegs mehrfach. Selbst das Beobachten (Monitoring) des ein- und ausgehenden Verkehrs auf einem solchen Server erlaubt so kaum noch Rückschlüsse über den Weg einzelner Nachrichten. Ein interessantes Programm, das es erleichtert, PGP und anonyme Remailer zu nutzen, ist Private Idaho (http://wkweb4.cableinet.co.uk/hmartin/pidaho.html) .

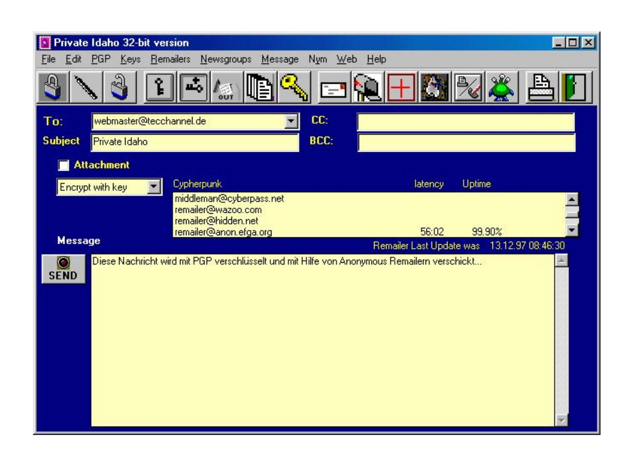


Bild 5: Private Idaho kombiniert PGP-Verschlüsselung und das Versenden über anonyme Remailer. Weg und Inhalt der Nachricht lassen sich so kaum enthüllen.

Ein relativ unkompliziertes, aber dennoch recht sicheres Verfahren mit echtem SMTP- und POP-Zugang bietet PrivacyX (http://www.privacyx.com/) . Die Kombination von digitaler Verschlüsselung und dem Weiterleitungsservice des PrivacyX-Servers verhindert, dass Unbefugte Ihre verschlüsselte Mail lesen oder mit einfachen technischen Mitteln zu Ihnen zurückverfolgen können. Der einzige Schwachpunkt, der neben dem bereits erwähnten Servermonitoring bleibt, ist PrivacyX selbst, das gegebenenfalls unter juristischem Druck die über Sie gespeicherten Daten offen legen muss. Da Sie für einen Account eine gültige E-Mail-Adresse angeben müssen, kann Ihnen also auch hier der Verlust der Anonymität drohen.

› Rechtsschutz gegen Datenmissbrauch

Das deutsche Recht schützt personenbezogene Daten in weitem Umfang. Ausschlaggebend ist § 3 des Teledienste-Datenschutzgesetzes (TDDSG), der die Verarbeitung personenbezogener Daten rechtlich fixiert. Diese ist danach nur zulässig, wenn der Betroffene in die Erhebung, Verarbeitung und Nutzung der Daten eingewilligt hat. Oder wenn es auf Grund des TDDSG explizit erlaubt ist. Explizit erlaubt ist nur eine ausschließlich zweckgebundene Verarbeitung von Daten. Alle Daten, die zur Durchführung des Vertrages nicht unbedingt gespeichert werden müssen, sind mit Beendigung der Verbindung zu löschen. Selbst wenn zunächst die Erfassung nötig war, um beispielsweise die Internetverbindung aufrecht zu erhalten.

Die Internet-Wirklichkeit sieht leider anders aus. Rechnerbezogene Daten werden laufend gesammelt. Darunter versteht man die Daten, die nicht einen einzelnen Benutzer, sondern einen einzelnen Computer eindeutig identifizieren. Die gesammelten Daten enthalten beispielsweise Informationen darüber, zu welcher Zeit einem Computer eine bestimmte IP-Adresse zugewiesen wurde. Oder wann ein bestimmter Computer welche Seite aufgerufen hat. Überprüfen können Sie dies etwa anhand der Historie-Liste im Internet Explorer, die zeigt, wann der Anwender welche Seiten besucht hat. Die Speicherung dieser Informationen in Cookies ermöglicht es, einen Rechner eindeutig zu identifizieren, was auf Grund der dynamischen IP-Adressvergabe sonst nicht möglich wäre.

› Daten sammeln ist erlaubt

Firmen dürfen anonymisierte Daten, also Daten, die keine Rückschlüsse auf eine einzelne Person erlauben, unbeschränkt sammeln. Datenschutzrechtliche Relevanz entsteht durch die Zusammenführung von rechnerbezogenen Daten mit personenbezogenen Daten. Zugang zu personenbezogenen Daten erhalten Firmen durch Anmeldungen oder Bestellungen des Benutzers. Firmen dürfen diese Daten nur zu dem Zweck nutzen, für den sie erhoben wurden.

Ein Beispiel ist die Onlinebestellung. Ihre Daten dürfen Firmen zur Durchführung einer Bestellung und zur Abrechnung speichern und nutzen. Diese Daten muss die Firma danach wieder löschen. Es sei denn, Sie geben ausdrücklich an, dass die Firma ihre Daten über einen längeren Zeitraum speichern soll. Etwa für den Fall, dass Sie laufend

Buchbestellungen aufgeben und Kreditkarten-Informationen nicht ständig neu übermitteln wollen. Erst dann ist die Speicherung Ihrer Angaben nach Durchführung der Bestellung weiter erlaubt.

Führen Firmen entgegen sämtlicher deutschen Datenschutzvorschriften rechnerbezogene Daten mit personenbezogenen Daten zusammen, entsteht der gläserne Internetuser, dessen Vorlieben und Benutzerverhalten sich werbewirksam ausnutzen lassen.

› Rechtliche Gegenmaßnahmen

Das TDDSG hat eine große Schwachstelle: Es enthält weder Buß- noch Strafvorschriften. Das bedeutet, dass es gegen Verstöße gegen die Bestimmungen des TDDSG keine staatlichen Sanktionen gibt. Die nächste Schwachstelle sind die deutschen Landesgrenzen. Außerhalb Deutschlands gilt das TDDSG nicht. In zahlreichen Ländern genießt der Datenschutz keinen so hohen Stellenwert hier zu Lande. Beispielsweise verbietet in den USA kein Datenschutzgesetz das Zusammenführen von rechner- und personenbezogenen Daten.

Man ist hier auf Gruppen angewiesen, die durch entsprechende Öffentlichkeitsarbeit die Datensammelwut mancher Firmen zu beschränken suchen. Diese Gruppen zielen darauf ab, die Firmen zur Selbstbeschränkung in Form von Privacy Policies zu zwingen. Jüngstes Beispiel ist die amerikanische Werbefirma DoubleClick, die auf diese Weise in die Schlagzeilen geraten ist (tecChannel berichtete (http://www.tecchannel.de/news/20000202/thema20000202-606.html)).

Im Gegensatz zu den USA und anderen Ländern besteht innerhalb der Europäischen Union theoretisch ein einheitlich hohes Datenschutzniveau. Dieses wurde durch die europäische Datenschutzrichtlinie festgelegt.

Ansprüche gegenüber Firmen

Sofern Sie den Verdacht haben, dass Ihre Daten missbraucht werden, können Sie gegenüber einer deutschen oder in der EU ansässigen Firma folgende Ansprüche geltend machen. Zunächst haben Sie einen Auskunftsanspruch darüber, welche Daten über Sie gespeichert sind und an wen die Firma diese Daten weitergegeben hat. Außerdem können Sie verlangen, dass die Firma Ihre Daten löscht.

Ist Ihnen durch die Weitergabe der Daten ein Schaden entstanden, so haben Sie weiter Anspruch auf Schadensersatz, wobei hier zweierlei problematisch ist.

Zunächst einmal müssen Sie einen konkreten Schaden nachweisen. Darüber hinaus müssen Sie einen Kausalzusammenhang zwischen der Weitergabe der Daten und dem eingetretenen Schaden herstellen können. Letzteres bedeutet, den Beweis zu führen, dass die unzulässige Weitergabe der Daten den eingetretenen Schaden jedenfalls mitverursacht hat.

› Fazit

Anonymes Surfen ist derzeit unmöglich. Zumindest Ihr Provider weiß genau, was Sie treiben, weil alle unverschlüsselten Daten, die Ihren Computer erreichen und verlassen, über seine Server fließen. Danach können Sie sich mit Anonymisierungs-Tools weitgehend unsichtbar machen, wobei die Betreiber der Tarn-Proxys als neue Mitwisser ins Spiel kommen. Eine verschlüsselte Verbindung zum Anonymisierer könnte den Provider eines Tages aus dieser Kette ausschließen.

Vergleichbares gilt beim Empfang und Versenden von E-Mail. Ihr Provider und der benutzte Dienst sind in der Lage, auf alle unverschlüsselten Informationen zuzugreifen. Die Empfangsstation ist ebenfalls ein potenzielles Sicherheitsloch. Einzig Verschlüsselungssoftware und/oder eine verschlüsselte Leitung zum E-Mail-Service können den Inhalt Ihrer Nachricht vor neugierigen Augen schützen.

Eine viel größere Gefahr droht in Zukunft von Software, die mit Ihrem Internetbesuch gar nichts zu tun hat. Ob Microsoft beim Online-Update mal eben die Konfiguration Ihres Computers ermittelt oder Reals Jukebox heimlich Ihre Musiksammlung katalogisiert und

per Internet weiterreicht: Sie können im Prinzip nichts dagegen tun, solange Sie nichts davon wissen. Jedes neue Programm erhöht das Risiko. Die zunehmende Nutzung des Internets für die Registrierung und für Produktupdates macht den Datenaustausch zwischen Software und Website zur Alltäglichkeit. Über die gleichzeitig "versehentlich" mitgelieferten Informationen kann man nur spekulieren. Die Einbindung in ein weltumspannendes Datennetz hat eben ihren Preis. (sda)

Rainer Wertenauer ist Rechtsanwalt in München und Fachanwalt für Arbeitsrecht.

Windows XP Bugs und Fixes

› Immer mehr Fehler tauchen in Windows XP auf - darunter häufig solche, die das Servicepack 1 erst verursacht. Wir zeigen Ihnen, was Sie gegen alte und neue Risiken unternehmen können.

› VON THOMAS RIESKE

Das Servicepack 1 (http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp) für Windows XP genießt einen schlechten Ruf. Kaum hatte Microsoft es im September 2002 veröffentlicht, beschwerten sich zahlreiche Anwender über massive Performance-Probleme nach der Installation. Programme starteten extrem langsam, und Dateien und Ordner ließen sich nur zäh über den Windows Explorer anzeigen, berichteten User. Einige konnten die eingebüßte Systemleistung zurückgewinnen, indem sie ihren On-Access-Virenscanner deaktivierten. Ähnliche Effekte gab es durch das Zusammenwirken des Servicepack und dem im Security Bulletin 03-013 (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-013.asp) erwähnten Kernel-Patch. Den immerhin hat Microsoft zwischenzeitlich nachgebessert.

Anwender, die trotzdem das Servicepack 1 installieren wollen, sollten also auf jeden Fall vorher ein Backup durchführen, um bei etwaigen Problemen den Ursprungszustand schnell wiederherstellen zu können. Weniger Wagemutige spielen nur die für sie relevanten Einzel-Patches auf, die Microsoft über die Seite Windows-Update (http://windowsupdate.microsoft.com) anbietet. Diese müssen Sie jedoch mit dem Internet Explorer unter Windows XP besuchen, damit Ihnen die Updates für dieses Betriebssystem überhaupt angezeigt werden. (mha/mec)

› Von SP1 behobene Probleme

Servicepack 1 behebt folgende Bugs (evtl. aufgeführte separate Patches gibt es weiterhin):

Sicherheitslücke im MUP

Der Windows-Dienst Multiple UNC Provider (MUP) spürt Netzwerkressourcen über deren UNC-Namen auf. Ein ungeprüfter Speicherbereich im MUP verursacht eine Sicherheitslücke.

Diese lässt sich über einen Pufferüberlauf ausnutzen, verursacht durch eine manipulierte Anfrage an den Dienst. Die Attacke löst entweder einen Neustart des Computers aus oder startet beliebige Programme im Sicherheitskontext des Betriebssystems.

Ein aktualisierter Treiber, den Microsoft zur Verfügung stellt, behebt den Fehler.

Sicherheitslücke im MUP

Datum	22.04.2002
Betrifft	Windows NT 4.0/2000/XP
Wirkung	Ausführen beliebigen Codes

Patch	in Deutsch
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase und Security Bulletin

› Keine vererbten Berechtigungen

Berechtigungen auf einem Server lassen sich remote über das Mapping eines Netzlaufwerks vergeben. Der Rechner, von dem aus der Administrator auf die Freigabe zugreift, interpretiert den verbundenen Share allerdings als Hauptverzeichnis. Dieses kennt per Definition kein darüber liegendes Verzeichnis, kann also auch keine Berechtigungen erben. Sind dennoch welche vorhanden, werden sie gelöscht.

Das Problem reicht laut Microsoft-Knowledgebase zurück bis Windows NT 4.0. Für diese Version gibt es allerdings nur einen Workaround: Entweder man vergibt die Berechtigungen direkt am Server oder meldet sich dort über die Terminal Services an. Die Patches für Windows 2000 und XP stellt Microsoft auf Anfrage zur Verfügung.

Keine vererbten Berechtigungen

Datum	23.10.2001
Betrifft	Windows NT 4.0/2000; Windows XP Home/Professional/64-Bit Edition
Wirkung	Vererbte Berechtigungen werden gelöscht
Patch	nur auf Anfrage bei Microsoft
Abhilfe	Patch installieren. Workaround: Berechtigungen direkt am Server vergeben oder über die Terminal-Dienste anmelden
Informationen	Microsoft Knowledgebase

› DoS-Angriff gegen UPnP-Dienst

Der unter Windows XP standardmäßig installierte Dienst "Universeller Plug & Play-Gerätehost" (UPnP) erweist sich als anfällig gegenüber einer bestimmten Befehlsfolge. Schickt ein Angreifer wiederholt solche Sequenzen an Rechner, auf denen der UPnP-Dienst läuft, wird immer mehr Speicher allokiert und nicht mehr freigegeben. Dieses Speicherleck sorgt dafür, dass die System-Performance einbricht und der Rechner schließlich nicht mehr reagiert - eine klassische DoS-Attacke also.

Von dem Bug ebenfalls betroffen sind Windows Me und alle Varianten von Windows 98. Letztere allerdings nur, falls der Anwender dort den Internet Connection Sharing Client von Windows XP installiert hat.

DoS-Angriff gegen UPnP -Dienst

Datum	22.10.2001
Betrifft	Windows Me, 98 / SE; Windows XP Home / Professional
Wirkung	DoS-Attacke
Patch	Über windowsupdate.microsoft.com
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase und Security Bulletin

› Applikations-Kompatibilität von XP

Beim Umstieg auf ein neues Betriebssystem möchten viele Anwender bereits vorhandene Software weiterhin einsetzen. Das ist für gängige Programme mittels

Kompatibilitätsmodus möglich. Die Liste der unterstützten Altapplikationen wird von Microsoft regelmäßig aktualisiert.

Das neueste Kompatibilitäts-Update datiert vom 8. April 2002 und enthält ebenfalls zwei bereits erschienene Updates. Damit lässt sich auch systemnahe Software wie McAfee VirusScan 5.16 und 5.21 oder der Nero UDF Reader für Nero 5.5 unter XP betreiben.

Applikations-Kompatibilität von XP

Datum	08.04.2002
Betrifft	Windows XP Home/Professional
Wirkung	Fehler und Abstürze bei älteren Programmen
Patch	über windowsupdate.microsoft.com
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Computer bleibt im Standby-Modus

Wenn der Rechner im Standby-Modus einfriert, ist daran womöglich ein älterer PCI-Treiber schuld. Dieser wartet beim Aufwachen aus dem Strom sparenden Zustand nicht die vorgeschriebenen 10 Millisekunden, bevor er ein Gerät anspricht.

Microsoft empfiehlt ein Update der Datei Pci.sys auf die Versionsnummer 5.1.2600.21.

Computer bleibt im Standby-Modus

Datum	16.01.2002
Betrifft	Windows XP Home/Professional
Wirkung	Rechner hängt sich auf
Patch	in Deutsch
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Absturz bei USV-Betrieb

Eine unterbrechungsfreie Stromversorgung (USV) soll zum einen die Qualität der Netzspannung erhöhen, zum anderen einen Stromausfall überbrücken. Daher schließt man an eine USV meist Geräte an, die hochverfügbar sein müssen, etwa Server in Rechenzentren.

Umso ärgerlicher ist es dann, wenn sich der unter Windows XP zuständige Dienst "Unterbrechungsfreie Stromversorgung" nicht starten lässt. Stattdessen erhält der Anwender eine Meldung über einen Anwendungsfehler in der Datei Ups.exe.

Absturz bei USV-Betrieb

Datum	22.10.2001
Betrifft	Windows XP Home / Professional
Wirkung	USV lässt sich nicht konfigurieren
Patch	Über windowsupdate.microsoft.com
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› IME verhindert korrektes Herunterfahren

Beim Herunterfahren des Rechners kann es passieren, dass Windows XP sich aufhängt.

Meist geschieht das während der Meldung "Einstellungen werden gespeichert". Hier hilft nur noch der Griff zum Aus-Schalter.

Der sporadisch auftretende Bug lässt sich auf den Input Method Editor (IME) zurückführen, wenn man ihn für die Verwendung während des Willkommens-Bildschirms eingerichtet hat.

Der Patch von Microsoft tauscht die Datei shgina.dll aus dem System32-Ordner des Betriebssystems aus.

IME verhindert korrektes Herunterfahren

Datum	22.10.2001
Betrifft	Windows XP Home/Professional
Wirkung	Windows hängt sich während des Herunterfahrens auf
Patch	Über windowsupdate.microsoft.com
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Internes Modem und XP

Wer vorhat, ein internes AC'97-Modem auf einem Notebook mit Intel-440MX-Chipsatz zu nutzen, sollte zuvor einige Aktualisierungen vornehmen. Ansonsten besteht die Gefahr, dass sich Windows XP aufhängt.

Um dem vorzubeugen, empfiehlt es sich, zunächst eine aktuelle BIOS-Version für das Notebook einzuspielen. Diese findet sich in der Regel auf den Internet-Seiten des jeweiligen Herstellers. Anschließend installiert man das Pentium-III-Update von der Seite Windows-Update (http://windowsupdate.microsoft.com) .

Im letzten Schritt muss der Anwender die Registry anpassen. Im Zweig HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ P3\ Parameters fügt man den DWORD-Wert HackFlags hinzu, der den Wert 1 (hexadezimal) erhält.

Internes Modem und XP

Datum	22.10.2001
Betrifft	Windows XP Home / Professional
Wirkung	XP hängt sich bei Gebrauch eines AC'97-Modems auf
Patch	Über windowsupdate.microsoft.com
Abhilfe	Patch installieren und Registry anpassen; zusätzlich BIOS-Update
Informationen	Microsoft Knowledgebase

› Installationsproblem über Funknetz

Funkgestützte Netzwerke (WLAN) als Alternative zu kabelgestützten LANs für kleine Netze oder als Ergänzung im Firmennetz liegen voll im Trend. Das Kabelgewirr auf dem Schreibtisch entfällt, und Rechner können auch "mobil" eingesetzt werden.

Doch der Fortschritt hat seine Tücken. Versucht man etwa, unter Windows XP Software zu installieren, die den Microsoft-Installer (MSI) nutzt, kann der Fehler 2229 auftreten. Dieses Verhalten wird vom MSI verursacht, dessen Fehler-Handling an Verbindungsaussetzern scheitert.

Einen Patch stellt Microsoft nur auf Anfrage zur Verfügung.

Installationsproblem über Funknetz

Datum	18.10.2001

Betrifft	Windows XP Home / Professional
Wirkung	Installation über WLAN bricht ab
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Langsame SCSI-Platten

Anwender, die in ein SCSI-System investieren, bezahlen dafür einen deutlich höheren Preis als für ein IDE-Pendant. Dafür erwarten sie dann aber auch mehr Leistung.

SCSI-Festplatten indes können ihren Geschwindigkeitsvorteil unter Windows XP mit NTFS-Dateisystem nicht ausspielen. Ihre Leistung liegt deutlich niedriger als erwartet. Das ist kein rein subjektiver Eindruck, sondern ein Bug im Treiber Ntfs.sys. Eine neue Version erhalten Betroffene auf Anfrage bei Microsoft.

Langsame SCSI-Platten

Datum	16.04.2002
Betrifft	Windows XP Home / Professional
Wirkung	Langsame SCSI-Festplatten nach XP-Installation
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› USB-2.0-Unterstützung

Viele waren verwundert, dass Windows XP ohne Unterstützung für den 480 Mbit/s schnellen Universal Serial Bus (USB) 2.0 auf den Markt kam. Doch diesen befand Microsoft, bis dato eifrigster Verfechter des neuen Standards, als zu wenig ausgereift.

Mittlerweile haben die Redmonder ihre Meinung revidiert, und XP-Benutzer können ihr Betriebssystem über ein Update nachrüsten.

USB-2.0-Unterstützung

Datum	11.04.2002
Betrifft	Windows XP Home / Professional
Wirkung	Keine USB-2.0-Unterstützung
Patch	Über windowsupdate.microsoft.com
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Kein Hinweis auf ablaufendes Passwort

In der Windows-Benutzerverwaltung lässt sich vorgeben, dass User ihr Kennwort regelmäßig wechseln müssen. Als Erinnerung erhalten sie einige Tage vor Ablauf des Termins bei der Anmeldung einen entsprechenden Hinweis. Dieser fehlt aber, wenn jemand sich mit einem XP-Rechner an einer Windows-2000-Domäne anmeldet.

Grund ist die standardmäßig aktivierte Anmelde-Optimierung. Sie bewirkt, dass XP während des Logon nicht wartet, bis die Netzwerkeinstellungen initialisiert sind. Stattdessen werden existierende User über die im Cache vorhandenen Anmelde-Informationen authentifiziert.

Einen Patch gibt es nur auf Anfrage bei Microsoft. Doch ein Workaround reicht auch:

Deaktivieren Sie einfach die Anmelde-Optimierung in der Management-Konsole für Gruppenrichtlinien. Dazu muss die Option "Computerkonfiguration\ Administrative Vorlagen\ System\ Anmeldung\ Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten" eingeschaltet sein.

Kein Hinweis auf ablaufendes Passwort

Datum	19.03.2002
Betrifft	Windows XP Professional
Wirkung	User erhalten keine Erinnerung, dass ihr Passwort abläuft
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Patch installieren. Workaround: Anmeldeoptimierung deaktivieren
Informationen	Microsoft Knowledgebase

› Bildschirmschoner verhindert Stromsparmodi

Gerade für Besitzer von tragbaren Rechnern sind die Stromsparmodi wichtig, sorgen sie doch für eine längere Akku-Laufzeit. Neben der Möglichkeit, separat Monitor und Festplatte Timer-gesteuert auszuschalten, bietet Windows einen Standby- und einen Ruhemodus.

In diese Energie sparenden Zustände wechselt der PC allerdings nicht, wenn ein Direct3D-basierter Bildschirmschoner, etwa 3D-FlowerBox oder 3D-Rohre, aktiv ist.

Ein Hotfix von Microsoft behebt diesen Fehler. Alternativ kann man auch auf andere Bildschirmschoner ausweichen.

Bildschirmschoner verhindert Stromsparmodi

Datum	07.03.2002
Betrifft	Windows XP Home / Professional
Wirkung	Rechner wechselt nicht in Energiesparmodi
Patch	in Deutsch
Abhilfe	Patch installieren oder auf andere Bildschirmschoner ausweichen
Informationen	Microsoft Knowledgebase

› Dynamic Update 1.2 auf Deutsch

Kein Bug, sondern eine wichtige Info für alle, die sich fragen, wie sie an die deutsche Version des Dynamic Update 1.2 kommen. Der Knowledgebase-Artikel Q314582 (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q314582) spricht nur von einer englischen Fassung. Doch ausgehend von dem dort angegebenen Download-Link lässt sich auf die URL für andere Sprachen schließen. Wir ersetzen in der Adresse EN-US durch DE und im Dateinamen ENU durch DEU - schon können wir das Update für das deutsche XP (http://download.microsoft.com/download/whistler/Patch/Q311542/WXP/DE/q311542_WXP_SP1_x86_DEU.exe) herunterladen.

Das Dynamic Update 1.2 enthält alle Fixes aus den Versionen 1.0 und 1.1. Außerdem beseitigt es die in Q312942 (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q312942) und Q314931 (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q314931) beschriebenen Bugs, die beim Upgrade auf Windows XP auftreten können.

Dynamic Update 1.2 auf Deutsch

Datum	06.02.2002

Betrifft	Windows XP Home / Professional
Wirkung	Dynamic Update 1.2 in Deutsch
Patch	in Deutsch
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Rechner wechselt nicht in Standby-Modus

Wer in den Energie(spar)optionen angibt, dass der Computer nach 45 oder mehr Minuten in den Standby-Modus wechselt, dürfte sich wundern: Dieser Zustand wird nie erreicht - falls der Rechner an einer Wechselspannung betrieben wird.

Schuld an diesem Verhalten ist der Idle Task Scheduler von Windows XP. Er startet nach 30 Minuten Inaktivität des Systems und setzt dabei den Inaktivitätszähler zurück.

Einen Patch für diesen Bug erhält man nur auf Anfrage bei Microsoft.

Rechner wechselt nicht in Standby-Modus

Datum	29.11.2001
Betrifft	Windows XP Home / Professional
Wirkung	Standby-Modus wird nach vorgegebener Zeit nicht aktiviert
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› PC-Cards werden nicht erkannt

PC-Cards (vormals PCMCIA), die unter Windows 98/Me/2000 noch problemlos funktionieren, erkennt Windows XP nicht. Stattdessen versieht der Geräte-Manager diese Devices mit einem Ausrufezeichen und weist ihnen keine Ressourcen zu.

Der Treiber Pcmcia.sys von Windows XP erkennt keine PC-Cards, die ihre Konfiguration im normalen PC-Card-Speicher ablegen. Vielmehr erwartet der Treiber diese Informationen in einem speziellen Bereich, dem "Attribute Memory".

Ein aktualisierter Treiber, den man jedoch nur auf Anfrage von Microsoft erhält, behebt diesen Bug.

PC-Cards werden nicht erkannt

Datum	21.11.2001
Betrifft	Windows XP Home / Professional
Wirkung	PC-Cards funktionieren nicht
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Zerstörte Daten bei OEM-Version

Wer einen neuen Rechner kauft, findet darauf häufig Windows XP als so genannte OEM-Version vorinstalliert. Datenverlust droht, wenn der Anwender:

- › Dateien in das bestehende XP-Verzeichnis neu einspielt (In-Place-Upgrade)
- › die Reparaturfunktion einsetzt oder

› ein Upgrade von der OEM-Home- auf die Retail-Professional-Edition durchführt

In diesen Fällen können Einstellungen unter "All Users" und "Default User" verloren gehen sowie die von Programmen gemeinsam genutzten Dateien beschädigt werden.

Einen Fix gibt es mit Stand 6. Juni 2002 nur für das englische XP. Besitzer anderer Sprachversionen müssen sich damit behelfen, die Datei undo_guimode.txt aus dem System32-Ordner des Betriebssystems zu löschen.

Zerstörte Daten bei OEM-Version

Datum	09.11.2001
Betrifft	Windows XP Home/Professional
Wirkung	Datenverlust
Patch	nur auf Englisch über windowsupdate.microsoft.com
Abhilfe	Englisches XP: Patch installieren. Workaround: Datei undo_guimode.txt löschen
Informationen	Microsoft Knowledgebase

› Keine Remote-Unterstützung

Mit Hilfe der Remote-Unterstützung kann ein Anwender andere Benutzer per E-Mail oder Instant Messenging um Hilfe bitten. Im Rahmen dieser Support-Maßnahmen lässt sich der PC des Hilfesuchenden auch fernsteuern - dessen Einverständnis vorausgesetzt. Gerade in größeren Unternehmen dürften die Help-Desk-Mitarbeiter solche Möglichkeiten zu schätzen wissen.

Unter gewissen Konstellationen ist es allerdings unmöglich, eine Remote-Sitzung zu starten. Dies gilt immer dann, wenn auf den miteinander kommunizierenden Computern Windows XP entweder als OEM-Version oder als Volumenlizenz vorinstalliert ist.

Microsoft hat für diesen Bug einen Patch bereitgestellt, der sich auch separat herunterladen lässt - unter anderem auf Deutsch.

Keine Remote-Unterstützung

Datum	08.11.2001
Betrifft	Windows XP Home / Professional
Wirkung	Remote-Unterstützung kann nicht gestartet werden
Patch	In Deutsch
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Keine Streams im Media Player

In der XP-Home-Edition kann es passieren, dass der Windows Media Player keinen Zugriff auf Multimedia-Streams zulässt. Das trifft für alle User mit eingeschränkten Rechten zu. Und zwar dann, wenn man das Anwenderprofil aus der bestehenden Datei usrclass.dat unter Default User kopiert. Ist noch kein Profil in usrclass.dat abgelegt, tritt der Fehler nicht auf.

Momentan gibt es noch keinen allgemein verfügbaren Fix, der den Fehler behebt. Als Workaround bietet sich lediglich an, auf das Kopieren eines Profils von usrclass.dat zu verzichten.

Keine Streams im Media Player

Datum	23.10.2001
Betrifft	Windows XP Home

Wirkung	Kein Zugriff auf Multimedia-Streams
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Patch installieren. Workaround: User-Profil nicht von usrclass.dat kopieren.
Informationen	Microsoft Knowledgebase

› Eingeschränkte Suchfunktion

Der Windows-Explorer erlaubt es, nicht nur nach dem Namen, sondern auch nach dem Inhalt von Dateien zu fahnden. Doch selbst wenn sie die gesuchten Zeichen enthalten, bleiben 76 Dateitypen unberücksichtigt, unter anderem solche mit den Endungen .css, .rtf und .xml.

Das liegt daran, dass für diese Dateien keine gültige Filterkomponente registriert ist. Abhilfe verspricht das Application Compatibility Update unter windowsupdate.microsoft.com (http://windowsupdate.microsoft.com) .

Eingeschränkte Suchfunktion

Datum	22.10.2001
Betrifft	Windows XP Home / Professional
Wirkung	Nicht alle Dateitypen werden nach ihrem Inhalt durchsucht
Patch	Über windowsupdate.microsoft.com
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Fehler im Migrationstool

Verschiedene Einstellungen von Betriebssystem und Applikationen lassen sich über den Transferassistenten von einem Rechner auf einen anderen übertragen. Die Daten des Quellsystems kann man beispielsweise auf einer Festplattenpartition oder einem Netzlaufwerk sammeln und darüber die Zielrechner versorgen. Auf diese Weise lässt sich etwa die Konfiguration für den Internet Explorer, Outlook (Express), den Windows-Desktop oder das DFÜ-Netzwerk übernehmen.

Das wäre alles ganz praktisch, wenn der zuständige Assistent in XP nicht einige Macken aufweisen würde. Selbst wenn der Wizard nicht bereits während des Transferprozesses abbricht, muss der Anwender mit einigen Überraschungen rechnen. So ist es etwa möglich, dass Icons auf dem Desktop anders als erwartet reagieren oder die Accounts in Outlook Express verloren gehen.

Für diesen Bug stellt Microsoft einen Patch auf der Windows-Update-Seite bereit.

Fehler im Migrationstool

Datum	22.10.2001
Betrifft	Windows XP Home / Professional
Wirkung	Einstellungen werden nicht übernommen
Patch	Über windowsupdate.microsoft.com
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Keine DVD-Wiedergabe

Viele DVDs, die mit Hilfe der Authoring-Lösung von Spruce Technologies erzeugt

werden, enthalten keine Nachschlagetabelle, über die der DVD-Player die Video-Sequenzen auf der Scheibe findet.

Der Versuch, eine solche DVD mit dem in XP integrierten Windows Media Player abzuspielen, führt zu einem Fehler. Die Wiedergabe der DVD wird nur kurz gestartet und unmittelbar danach abgebrochen.

Microsoft stellt einen Patch zur Verfügung, der die Datei Qdvd.dll austauscht.

Keine DVD-Wiedergabe

Datum	22.10.2001
Betrifft	Windows XP Home / Professional
Wirkung	DVD kann nicht abgespielt werden
Patch	Über windowsupdate.microsoft.com
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Störgeräusche durch USB-Audio-Treiber

Der Treiber Usbuhci.sys ist schuld daran, wenn der Audio-Genuss über USB-Boxen durch Störgeräusche unterbrochen wird. Die Störungen treten dabei im Sekunden- oder Minutentakt auf.

Wer den aktualisierten Treiber nicht gleich bei der XP-Installation über das "Dynamic Update" einbindet, kann dies auch später über das Download Center nachholen.

Störgeräusche durch USB-Audio-Treiber

Datum	18.10.2001
Betrifft	Windows XP Home / Professional
Wirkung	Störgeräusche bei Audio-Wiedergabe über USB-Boxen
Patch	Über "Dynamic Update" während der Installation; später über das Download Center
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Stromsparmodus PowerNow! funktioniert nicht

AMD bietet mit PowerNow! eine Stromspartechnik für seine Notebook-CPUs. Mit diesem Feature lassen sich Takt und Spannung dynamisch je nach Auslastung des Systems reduzieren, um so die aufgenommene Leistung zu reduzieren.

Diese Funktionalität kann Windows XP erst nutzen, wenn der Anwender einen separaten Treiber installiert. Doch allein damit ist es nicht getan, denn zusätzlich muss man die Registry anpassen:

Im Zweig HKEY_LOCAL_MACHINE\ System\ CurrentControlSet \ Services\ AmdK7\ Parameters fügt man einen DWORD-Wert hinzu. Dieser erhält den Namen HackFlags und den hexadezimalen Wert 1. Damit ist PowerNow! nach dem nächsten Neustart aktiv.

Stromsparmodus PowerNow! funktioniert nicht

Datum	15.10.2001
Betrifft	Windows XP Home / Professional
Wirkung	AMDs Stromspar-Feature PowerNow! wird nicht aktiviert
Patch	Auf Deutsch

Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Neu: Leck im HTML-Konverter

Windows verfügt über einen integrierten Konverter, der dafür sorgt, dass Anwender Dateien im HTML-Format anzeigen, importieren oder speichern können. Eine speziell präparierte Anfrage an die Konvertierroutine bewirkt einen Pufferüberlauf.

Diesen Fehler kann ein Angreifer ausnutzen, um Code mit den Rechten des angemeldeten Users auszuführen. Da sowohl der Internet Explorer als auch Outlook (Express) den HTML-Konverter nutzen, lässt sich eine solche Attacke über eine Webseite oder eine E-Mail durchführen.

Microsoft stellt Patches für alle betroffenen Windows-Versionen zur Verfügung.

Leck im HTML-Konverter

Datum	09.07.2003
Betrifft	Windows 98/Me/NT 4.0/2000/XP/Server 2003
Wirkung	Ausführen beliebigen Codes
Patch	Windows XP 32 Bit, Windows XP 64 Bit
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase und Security Bulletin

› Neu: Pufferüberlauf beim Message Handling

Ein Sicherheitsleck im Windows-Kernel ermöglicht es einem Angreifer, beliebigen Code auszuführen. Die Ursache dafür liegt im fehlerhaften Verfahren, mit dem der Kernel Nachrichten an einen Debugger weiterreicht.

Auf diese Weise lassen sich ohne Wissen des Anwenders etwa Accounts mit Administrator-Privilegien anlegen. Um die Lücke ausnutzen zu können, muss ein Angreifer jedoch lokalen Zugang zu der Maschine haben oder über eine Terminal-Session mit dem System verbunden sein.

Der Original-Patch, den Microsoft am 16. April 2003 veröffentlicht hat, ist fehlerhaft: Installiert man ihn auf XP-Systemen mit vorhandenem Servicepack 1, verursacht dies massive Performance-Einbußen. Abhilfe schafft der aktualisierte Bugfix vom 28. Mai 2003.

Pufferüberlauf beim Message Handling

Datum	16.04.2003
Betrifft	Windows NT 4.0/2000/XP
Wirkung	Ausführen beliebigen Codes
Patch	Windows XP 32 Bit; Windows XP 64 Bit
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase und Security Bulletin

› Neu: Sicherheitslücke in Microsofts Java Virtual Machine

Durch einen Bug in der Java Virtual Machine (JVM) von Microsoft kann ein Hacker beliebigen Code auf einem angegriffenen System ausführen. Verantwortlich für das Leck ist der Byte Code Verifier, eine Komponente der JVM, der eine bestimmte Codesequenz nicht korrekt prüft, so dass auch die folgenden Sicherheits-Checks versagen. Über ein entsprechend konstruiertes Java-Applet, etwa auf einer Website, kann ein Angreifer Code

mit den Rechten des lokal angemeldeten Users ausführen.

Für die betroffenen Versionen der JVM stellt Microsoft einen Patch über die Seite Windows Update bereit.

Sicherheitslücke in Microsofts Java Virtual Machine

Datum	09.04.2003
Betrifft	Alle Windows-Versionen mit der Microsoft JVM bis einschließlich Build 5.0.3809
Wirkung	Ausführen beliebigen Codes
Patch	Über die Seite Windows Update
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase und Security Bulletin

› Neu: DoS-Attacke über RPC

Eine Schwachstelle im RPC-Protokoll von Windows ermöglicht DoS-Angriffe. Die Komponente des Protokolls, die für den Nachrichtenaustausch über TCP/IP zuständig ist, lässt sich mittels manipulierter Datenpakete auf Port 135 zum Absturz bringen. Infolgedessen wird nicht nur der RPC-Dienst lahm gelegt, auch COM-Funktionen sind möglicherweise betroffen.

Microsoft stellt Patches für Windows 2000 und XP zur Verfügung. NT-Nutzer müssen hingegen auf einen Workaround zurückgreifen und Port 135 auf der Firewall blockieren.

DoS-Attacke über RPC

Datum	26.03.2003
Betrifft	Windows NT 4.0/2000/XP
Wirkung	Denial-of-Service-Attacke
Patch	Windows XP 32 Bit; Windows XP 64 Bit
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase und Security Bulletin

› Neu: Windows Explorer verursacht Anwendungsfehler

Wenn man versucht, mit dem Windows Explorer einen Ordner zu öffnen oder zu schließen, bewirkt dies einen Anwendungsfehler. Eventuell funktioniert beim erneuten Start von Explorer.exe aber alles wieder problemlos.

Wer dieses Vabanque-Spiel vermeiden will, greift zu einem Patch, der die Datei Duser.dll gegen eine neue Version austauscht.

Windows Explorer verursacht Anwendungsfehler

Datum	22.04.2003
Betrifft	Windows XP Home/Professional
Wirkung	Windows Explorer stürzt ab
Patch	in Deutsch
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Setup und Asus P2B Motherboard

Kleine Ursache, große Wirkung: Das gilt auch für ein Problem, das im Zusammenhang

mit dem Asus (http://www.asuscom.de/) -Mainboard P2B auftritt. Auf Rechnern, die eine Hauptplatine dieses Typs besitzen, lässt sich XP zwar problemlos installieren. Der anschließende Start des Betriebssystems geht allerdings schief: Der Computer hängt sich auf, und der Task-Manager gibt an, dass die CPU 100 Prozent der Systemressourcen beansprucht.

Der von Microsoft angegebene Workaround ist simpel: Der Anwender muss lediglich im Rechner-BIOS die Option "Wake up if mouse is moved" deaktivieren.

Setup und Asus P2B Motherboard

Datum	17.10.2001
Betrifft	Windows XP Home / Professional / 64-Bit-Edition
Wirkung	Rechner stürzt ab
Patch	Nicht verfügbar
Abhilfe	BIOS-Option "Wake up if mouse is moved" deaktivieren
Informationen	Microsoft Knowledgebase

› Upgrade von Windows 98 / Me schlägt fehl

Wer sich entschließt, ein Upgrade von Windows 98/SE oder Windows Me durchzuführen, sollte vorab den Inhalt des Windows-Unterverzeichnisses System32\ Catroot2 löschen. Die dort enthaltenen Dateien sollte eigentlich die XP-Installationsroutine entsorgen, doch mitunter erledigt sie diese Aufgabe nicht.

Stattdessen begrüßt den Anwender eine kryptische Fehlermeldung, die den Error Code fffffdf0 auf Grund einer vermeintlich ungültigen Signatur des XP-Setup ausgibt. Außerdem erfährt man, dass das System den Text für Nachricht Nummer 0xfffffdf0 im Message File für die Syssetup.dll nicht finden kann. Ob der Benutzer damit etwas anfangen kann oder nicht - die Installation bricht nach der Meldung ab, und der Computer wird permanent neu gestartet.

Upgrade von Windows 98 / Me schlägt fehl

Datum	05.10.2001
Betrifft	Windows XP Home / Professional
Wirkung	Upgrade lässt sich nicht durchführen
Patch	Nicht verfügbar
Abhilfe	Manuelles Löschen von Dateien
Informationen	Microsoft Knowledgebase

› XP-Setup hängt bei Installation unter Windows 95

Führt man das XP-Setup unter Windows 95 aus und wählt die Option "Neuinstallation", hängt sich die Installationsroutine auf. Im Dialogfeld "Setupoptionen" kann der Anwender zwar noch auf "Weiter" klicken, doch nach der Meldung "Installation abgeschlossen in ungefähr 52 Minuten" wird der Vorgang nicht fortgesetzt. Als einzige Möglichkeit bleibt, das Setup-Programm abzubrechen.

Als Ursache gibt Microsoft an, dass unter Windows 95 die Anzahl möglicher Assistentenseiten begrenzt ist. Um das Problem zu umgehen, soll der Anwender eine beliebige Version des Internet Explorer unter Windows 95 installieren und anschließend das Windows-XP-Setup-Programm erneut ausführen. Alternativ dazu kann man auch den Computer von der XP-CD booten und dann die Installation starten.

XP-Setup hängt bei Installation unter Windows 95

Datum	13.09.2001

Betrifft	Windows XP Home / Professional
Wirkung	XP-Setup kann nicht durchgeführt werden
Patch	Nicht verfügbar
Abhilfe	Beliebige IE-Version unter Win95 installieren oder von XP-CD booten und Installation starten
Informationen	Microsoft Knowledgebase

› XP-Setup unter DOS hängt sich auf

Es gibt durchaus gute Gründe, das XP-Setup von der DOS-Kommandozeile aus zu starten. Etwa dann, wenn man einen Rechner komplett neu aufsetzen will und das BIOS kein Booten von CD zulässt.

In diesem Fall lässt sich die Installationsroutine über die Datei winnt.exe aufrufen, die sich auf der Programm-CD im Verzeichnis \ i386 befindet. Das Setup kann sich allerdings aufhängen, wenn der Anwender zuvor nicht das Cache-Programm Smartdrive geladen hat. Bei dessen Aufruf sollte man auf Parameter verzichten, sonst droht ebenfalls ein Absturz - in unserem Versuch mit permanentem Festplattenzugriff.

XP-Setup unter DOS hängt sich auf

Datum	17.05.2001
Betrifft	Windows XP Home / Professional
Wirkung	Setup vom DOS-Prompt lässt sich nicht durchführen
Patch	Nicht verfügbar
Abhilfe	Smartdrive ohne Parameter laden
Informationen	Microsoft Knowledgebase

› NTLDR nicht vorhanden

Ob man XP im Parallelbetrieb mit Windows 9x installieren oder die betagteren Betriebssystemversionen aktualisieren will: In beiden Fällen kann es beim Setup nach dem ersten Reboot die Fehlermeldung geben: "NTLDR fehlt. Neustart mit beliebiger Taste."

Dieses Problem tritt nur auf, wenn Windows 9x auf einem FAT32-Laufwerk installiert ist. Der im FAT32-BIOS-Parameterblock (BPB) eingetragene Wert für die Köpfe der Festplatte passt nicht zur Geometrie des physischen Laufwerks. Das kann etwa durch einen missglückten Clone-Vorgang hervorgerufen worden sein. Der Windows 9x-Startcode ignoriert den Wert für die Köpfe im BPB und startet auch bei ungültigen Angaben. Windows XP und 2000 reagieren in dem Fall jedoch sensibler und starten nicht mehr.

Um den ungültigen Wert im FAT32-BPB zu korrigieren, ist es am einfachsten, den Windows-9x-Startcode neu zu schreiben. Dies gelingt über den Befehl "sys c:" Danach sollte die Installation von XP problemlos gelingen.

NTLDR nicht vorhanden

Datum	25.02.2000
Betrifft	Windows 2000; Windows XP Home / Professional
Wirkung	Rechner hängt nach Upgrade auf Windows 2000 / XP
Patch	Nicht verfügbar
Abhilfe	Windows-9x-Startcode neu schreiben (sys c:)
Informationen	Microsoft Knowledgebase

› Neu: Fehlende USB-2.0-Geräte

Windows XP mit installiertem Servicepack 1 sorgt für eine unangenehme Überraschung: Beim Aufwachen aus dem Ruhezustand erkennt das System bestimmte USB-2.0-Geräte nicht mehr. Obwohl sie nach wie vor angeschlossen sind, fehlen die Devices im Geräte-Manager.

Nach Aussage von Microsoft betrifft der Bug Geräte, die über die USB-2.0-Interfaces CY7C68013 oder CY7C68300 von Cypress verfügen.

Ein entsprechender Patch ist nur auf Anfrage beim (kostenpflichtigen) Support zu erhalten. Der Fehler lässt sich umgehen, indem Sie den Ruhezustand deaktivieren oder auf das Servicepack 1 verzichten.

Fehlende USB-2.0-Geräte

Datum	26.06.2003
Betrifft	Windows XP Home/Professional/64-Bit-Edition/Tablet-PC-Edition/Media Center-Edition
Wirkung	USB-2.0-Geräte funktionieren nach dem Aufwachen aus dem Ruhezustand nicht mehr.
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Patch installieren. Workaround: Ruhezustand deaktivieren oder auf Servicepack 1 verzichten
Informationen	Microsoft Knowledgebase

› Neu: Wechsel in Standby- oder Ruhemodus beschädigt Daten auf Festplatte

Um die volle Kapazität von ATA-Festplatten mit mehr als 137 GByte zu nutzen, kommt das 48-Bit-LBA-Verfahren zum Einsatz. Windows XP unterstützt dies mit dem Servicepack 1 - allerdings nicht in allen Situationen.

So verzichtet das Betriebssystem auf das moderne Adressierungsverfahren, wenn es ein Speicherabbild oder die Datei für den Ruhezustand anlegt. Außerdem vergisst Windows beim Wechsel in die Stromsparmodi, den Festplatten-Cache zu leeren.

Der Bug lässt sich über einen Microsoft-Patch beheben.

Wechsel in Standby- oder Ruhemodus beschädigt Festplatte

Datum	06.06.2003
Betrifft	Windows XP Home/Professional/64-Bit-Edition/Tablet-PC-Edition/Media Center-Edition
Wirkung	Korrupte Daten; instabiles System
Patch	Windows XP 32 Bit, Windows XP 64 Bit
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Neu: CD-Brenner wird nicht als Aufnahmegerät erkannt

Windows XP verfügt über eine integrierte Funktion zum Brennen von CDs. Mitunter passiert es jedoch, dass das Betriebssystem die vorhandenen CD-R- oder CD-RW-Laufwerke falsch identifiziert. In diesem Fall fehlt im Eigenschaftendialog der Laufwerke die Registerkarte "Aufnahme".

Das Problem lässt sich durch eine Änderung in der Registry beseitigen.

Im Zweig *HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ CD Burning\ Drives* finden Sie den Unterschlüssel *Volume{GUID}*. Bei GUID handelt es sich um eine hexadezimale Kennung pro Laufwerk. Tragen Sie im Feld "Drive Type" den Wert 1 für ein CD-R- und 2 für ein CD-RW-Laufwerk ein.

CD-Brenner wird nicht als Aufnahmegerät erkannt

Datum	06.08.2002
Betrifft	Windows XP Home/Professionell
Wirkung	CDs lassen sich mit der in XP integrierten Brennfunktion nicht beschreiben
Patch	Nicht verfügbar
Abhilfe	Registry modifizieren
Informationen	Microsoft Knowledgebase

› Fehlende Daten auf selbst gebrannter CD

Wer vorhat, CDs zu brennen, sollte dafür nicht gerade Windows XP bemühen: Die möglichen Resultate scheinen weit gehend vom Zufall abhängig. Dabei spielt es keine Rolle, ob man als Medium CD-Rs oder CD-RWs verwendet.

Entweder gelingt das Brennen der Daten überhaupt nicht. Oder die CD lässt sich nur unter Windows XP, nicht aber unter 9x lesen. Wie sich Windows 2000 verhält, verrät die Microsoft Knowledgebase nicht.

Außerdem kann es zu Datenverlust kommen: Fügt man der CD eine Datei hinzu, deren Name dem eines bereits vorhandenen Ordners entspricht, wird dieser gelöscht. Andersherum funktioniert das ebenfalls: Fügt man einen Ordner hinzu, dessen Name dem einer bereits vorhandenen Datei entspricht, wird die Datei gelöscht.

Einen Fix für dieses sonderbare Verhalten gibt es über das Microsoft Download Center.

Fehlende Daten auf selbst gebrannter CD

Datum	22.10.2001
Betrifft	Windows XP Home / Professional
Wirkung	CD nicht lesbar; Datenverlust
Patch	Auf Deutsch
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Weitere Themen zu diesem Artikel:

Windows-Update unter der Lupe (http://www.tecchannel.de/betriebssysteme/1125/index.html)
XP-Aktivierung per Internet entschlüsselt (http://www.tecchannel.de/betriebssysteme/1215/index.html)
Der Aktivierung auf der Spur (http://www.tecchannel.de/betriebssysteme/788/index.html)
Windows-Produkt-Aktivierung ausgehebelt (http://www.tecchannel.de/betriebssysteme/743/index.html)
Windows XP Final (http://www.tecchannel.de/betriebssysteme/602/index.html)
Windows XP Benchmarks (http://www.tecchannel.de/betriebssysteme/772/index.html)
Windows 2000 Bugs und Fixes (http://www.tecchannel.de/betriebssysteme/317/index.html)
Windows NT Bugreport (http://www.tecchannel.de/betriebssysteme/172/index.html)

Windows Me Bugreport (http://www.tecchannel.de/betriebssysteme/610/index.html)
Windows 98 Bugreport (http://www.tecchannel.de/betriebssysteme/79/index.html)

Windows 2000: Bugs und Fixes

› Wer meint, mit dem Servicepack 4 auf der sicheren Seite zu sein, der irrt. Etliche Fehler hat MS nicht behoben, neue Bugs sind inzwischen hinzugekommen. Wir nennen Ihnen die passenden Fixes und Workarounds.

› VON MIKE HARTMANN UND THOMAS RIESKE

Das seit Juni 2003 (http://www.tecchannel.de/news/20030627/thema20030627-11076.html) verfügbare Servicepack 4 (http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/) räumt mit einer Menge von Windows-2000-Fehlern auf. Eine Übersicht dazu gibt Microsoft in einem eigenen Knowledgebase-Artikel (http://support.microsoft.com/?kbid=327194) .

Wer sein System auf dem aktuellen Stand halten will, kommt um einen regelmäßigen Besuch der verschiedenen Microsoft-Download-Seiten nicht herum. Leider sind die Bugfixes und Updates für Windows 2000 nicht so einfach über den FTP-Server zu holen wie für Windows NT (http://www.tecchannel.de/betriebssysteme/172/index.html) . Wichtige Informationen finden sich verteilt auf die Windows-2000-Download-Seite (http://www.microsoft.com/windows2000/downloads/) , die Security-Bulletins (http://www.microsoft.com/technet/security/current.asp) und auf das Windows-Update (http://windowsupdate.microsoft.com/) . Die zuletzt genannte Seite müssen Sie allerdings mit einem Internet Explorer unter Windows 2000 besuchen, damit Ihnen auch die Updates für Windows 2000 angezeigt werden.

Im Gegensatz zu Windows NT lassen sich englische Patches für Windows 2000 nicht auf der deutschen Version aufspielen, selbst wenn das betroffene Programm nicht von der Sprachversion abhängig ist. Der Hotfix verweigert schlichtweg die Installation. Viele Administratoren bevorzugen deshalb die englische Version von Windows 2000, weil so wichtige Fehlerkorrekturen früher zur Verfügung stehen.

› Aktuell verfügbare Downloads

Seit Juni 2003 (http://www.tecchannel.de/news/20030627/thema20030627-11076.html) ist das Servicepack 4 (http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/) für Windows 2000 verfügbar. Das knapp 128 MByte große Archiv enthält alle Fixes aus den ersten drei Servicepacks und dem Security Rollup Package sowie weitere 650 Fehlerbereinigungen. Benutzer, die zuvor kein Service Pack (SP) installiert haben, sind nach Angaben von Microsoft mit Service Pack 4 komplett bedient. Wie viele zusätzliche Bugs im Rahmen der Codeüberprüfung intern gefunden wurden, von denen die Anwender gar nicht erst erfahren, steht in den Sternen.

Dennoch bleibt eine ganze Reihe von Bugs auch weiterhin unbehandelt, wie Sie der folgenden Liste entnehmen. Für diese müssen sich die Anwender mit Workarounds und einzelnen Patches begnügen. Zumindest können Sie damit allen in diesem Artikel vorgestellten Fehlern zu Leibe rücken.

Die Bugliste auf den folgenden Seiten zeigt jeweils an, auf welche Version von Windows 2000 der beschriebene Bug zutrifft. P steht für Professional, S für Server und AS für Advanced Server. Tritt der Bug nur in Zusammenhang mit einer bestimmten Software oder Komponente auf, so ist dies ebenfalls verzeichnet. (mha/mec)

› Neu: Von SP4 behobene Fehler

Servicepack 4 behebt nachfolgend beschriebene Bugs (eventuell aufgeführte separate Patches gibt es weiterhin):

Rechteausweitung im Netzwerkverbindungs-Manager

Der Netzwerkverbindungs-Manager ruft bei einer neuen Verbindung einen so genannten Handler auf. Das ist eine Routine, die normalerweise im Sicherheitskontext des Benutzers läuft. Der Bug allerdings ermöglicht es einem Angreifer, eigenen Code als Handler im Kontext LocalSystem ausführen zu lassen, also mit vollen Privilegien.

Ein entsprechender Patch ist bereits verfügbar und sollte so bald wie möglich eingespielt werden. Die entsprechende Datei Netman.dll läuft nur unter Windows 2000 mit Servicepack 2 oder 3 und hat die Version 5.0.2195.5974.

Rechteausweitung im Netzwerkverbindungs-Manager

Datum	23.07.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Hacker kann sich Rechte als LocalSystem verschaffen
Patch	In Deutsch
Abhilfe	Patch installieren
Infos	Microsoft Knowledgebase

› Kritischer Fehler im Zertifikatmanager

Ein Fehler bei der Validierung von Zertifikatsketten führt dazu, dass ein Angreifer eine falsche Identität vortäuschen kann, etwa bei SSL -Webseiten, unterschriebenen E-Mails, bei Anmeldeverfahren, die auf Zertifikaten basieren, oder im schlimmsten Fall bei zu installierenden Programmen.

Microsoft hat einen Patch bereitgestellt, den jeder Anwender sofort installieren sollte. Einen kleinen Nachteil hat der Patch allerdings: Nach der Installation behauptet Windows von allen Hardware-Treibern, dass sie den Windows-Logo-Test nicht bestanden haben. Ursache hierfür ist das für die Treiber verwendete Zertifikat, das nun nicht mehr vom System anerkannt wird.

Ist Windows so konfiguriert, dass nur zertifizierte Treiber installiert werden dürfen, lässt sich nun überhaupt kein neuer Treiber mehr einrichten. Dieses Verhalten können Sie in den Systemeigenschaften / Hardware / Treibersignierung umstellen.

Kritischer Fehler im Zertifikatmanager

Datum	04.09.2002
Betrifft	Alle Windows-Versionen
Wirkung	Angreifer kann falsche Identität vortäuschen
Patch	In Deutsch
Abhilfe	Patch installieren
Infos	Microsoft Knowledgebase

› Löschung von Zertifikaten

Ein spezielles ActiveX-Control ist in allen Windows-Versionen dafür zuständig, webbasierte Zertifikate in den lokalen Zertifikatsspeicher des Benutzers einzutragen. Ein Fehler in diesem Control ermöglicht es allerdings - in einem laut Microsoft sehr aufwendigen und komplizierten Verfahren -, auch Zertifikate vom lokalen System zu

löschen.

Das kann unangenehme Folgen haben, etwa wenn Root-Zertifikate oder für die EFS-Verschlüsselung zuständige Zertifikate plötzlich weg sind.

Ein entsprechend aktualisiertes Control ist von Microsoft verfügbar und sollte sofort installiert werden. Unter Windows 2000 und XP behebt dieser Patch auch gleichzeitig einen Fehler im ActiveX-Control, das für die Registrierung von SmartCards zuständig ist.

Löschung von Zertifikaten

Datum	28.08.2002
Betrifft	Alle Windows-Versionen
Wirkung	Zertifikate können ungewollt gelöscht werden
Patch	In Deutsch
Abhilfe	Patch installieren
Infos	Microsoft Knowledgebase

› WebDAV-Anfragen immer im User-Kontext

Mit WebDAV, einer Erweiterung von HTTP, lassen sich Webinhalte von einem entfernten Standort aus erstellen und verwalten. Die Komponente in Microsoft-Produkten, die den Zugriff auf WebDAV-Ressourcen ermöglicht, heißt Internet Publishing Provider (IPP). Der IPP sollte Anfragen des Anwenders von Anfragen durch ein Script, das im Browser abläuft, unterscheiden können.

Genau diese Unterscheidung findet durch einen Implementierungsfehler aber nicht statt: Der IPP behandelt alle Anfragen im Sicherheitskontext des Users. Von dessen Berechtigungen hängt es also ab, welchen Schaden ein Angreifer über diese Lücke verursachen kann. Denkbar wäre beispielsweise ein Zugriff aufs Intranet oder auf webbasierte E-Mail.

WebDAV-Anfragen immer im User-Kontext

Datum	18.04.2001
Betrifft	Windows 9x, Me, NT, 2000
Wirkung	Zugriff auf User-Daten
Patch	Windows Security Patch
Abhilfe	Patch installieren
Informationen	Microsoft Security Bulletin

› Bluescreen bei NAT und VPN

Ein Windows-2000-Server, der parallel zu Routing und Remote-Access auch NAT (Network Address Translation) und VPN (Virtual Private Network) anbietet, bleibt mit einer STOP-Meldung stehen. Der Grund ist, dass ein IP-Paket durch NAT aktualisiert wird, aber nicht der Referenzzähler für die Routen. Darum kann die für das Aufräumen zuständige Routine nicht korrekt funktionieren und das System bleibt stehen.

Es gibt zwar einen Fix von Microsoft, doch ist dieser nur über den (kostenpflichtigen) Support erhältlich. Bis zur Veröffentlichung des Fixes bleibt bloß, den NAT-Dienst auf einen anderen Server zu verschieben, der keine VPN-Verbindungen annimmt.

Bluescreen bei NAT und VPN

Datum	18.02.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	STOP-Meldung

Patch	Nur auf Anfrage bei Microsoft
Abhilfe	NAT-Dienste auf anderen Server verschieben
Infos	Microsoft Knowledgebase

› Rechner hängt beim Aufwachen aus Standby

Beim Aufwachen aus dem Standby-Modus (S3 Deep-Sleep) kann der Rechner abstürzen, wenn zwei IDE-Laufwerke an einem Kabel hängen. Das liegt daran, dass der Treiber das Busy-Signal des Laufwerks nicht überprüft, bevor er das Reset-Kommando schickt. Dadurch werden die beiden Laufwerke beim Neustart zurückgesetzt, ehe die Synchronisierung abgeschlossen ist.

Zwar müsste laut ATAPI-Spezifikation das Laufwerk das Reset-Signal ignorieren, solange es noch beschäftigt ist, aber manche tun das nicht.

Es gibt zwar einen Fix von Microsoft, der den Treiber veranlasst, das Busy-Signal zu respektieren, doch ist dieser nur über den (kostenpflichtigen) Support erhältlich. Ein Workaround für Betroffene ist das Verteilen der Laufwerke auf die beiden IDE-Kanäle.

Rechner hängt beim Aufwachen aus Standby

Datum	16.04.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Beim Aufwachen aus Standby stürzt Rechner ab
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Laufwerke auf IDE-Kanäle verteilen
Infos	Microsoft Knowledgebase

› TURN killt SMTP-Server

Mit einem einfachen TURN-Befehl (RFC 821) kann man in einer Telnet-Sitzung den SMTP-Dienst von Windows 2000 abschießen. Normalerweise dient TURN in einer SMTP-Session dazu, die Rollen der beiden beteiligten Server zu verkehren - der Sender wird zum Empfänger und umgekehrt.

Ein böswilliger User kann den Bug zu einer DoS-Attacke nutzen, indem er sich einfach per Telnet mit dem SMTP-Dienst von Windows 2000 verbindet und das Kommando TURN schickt.

Ein Patch ist - wie so oft - nur über den (kostenpflichtigen) Support zu erhalten. Bis zur allgemeinen Verfügbarkeit empfiehlt sich die Verwendung eines anderen SMTP-Dienstes nach außen.

TURN killt SMTP-Server

Datum	18.05.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	SMTP-Dienst bleibt stehen
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Anderen SMTP-Dienst verwenden
Infos	Microsoft Knowledgebase

› Zugriffsverletzung im Drucker-Spooler

Ein Fehler in der Tcpmib.dll führt dazu, dass ein mittels SNMP verwalteter Druckserver unter Windows 2000 eine Schutzverletzung im Programm Spoolsv.exe verursacht. Danach steht die Druckwarteschlange auf diesem Server nicht mehr zur Verfügung, und

es kann nicht mehr gedruckt werden.

Eine aktualisierte Tcpmib.dll gibt es nur beim kostenpflichtigen Support.

Zugriffsverletzung im Drucker-Spooler

Datum	07.08.2002
Betrifft	Windows 2000 P, S, AS; SNMP
Wirkung	Schutzverletzung
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Druckwarteschlange nicht per SNMP verwalten
Infos	Microsoft Knowledgebase

› Speichermedien verlieren Daten während Hibernation

Besitzern von Digitalkameras könnte etwas Ähnliches schon einmal passiert sein. Sie haben ein Speichermedium (http://www.tecchannel.de/hardware/303/index.html) wie Compact Flash, Memory Stick oder Smart Media im Rechner eingelegt, Windows 2000 in den Ruhezustand versetzt und dann das Medium aus dem Rechner entfernt, um neue Aufnahmen zu machen. Wenn Sie danach das Medium erneut in den Rechner einlegen und ihn starten, befindet sich der alte Inhalt auf dem Medium - von den neuen Daten keine Spur. Das liegt daran, dass Windows 2000 beim Wechsel in den Ruhezustand den Inhalt des Mediums cached und dann wieder einspielt.

Ein Patch ist derzeit nur beim kostenpflichtigen Support verfügbar. In der Zwischenzeit empfiehlt es sich, zunächst den Rechner hochzufahren und erst dann das Medium einzulegen.

Speichermedien verlieren Daten während Hibernation

Datum	29.07.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Daten verschwinden von Speichermedien
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Erst Rechner starten, dann Medium einlegen
Infos	Microsoft Knowledgebase

› Neue AGP-Karte auf Board mit VIA-Chipsatz

Der Einbau einer neuen AGP-Grafikkarte in einen Rechner mit VIA-Chipsatz kann dazu führen, dass das System beim nächsten Start hängen bleibt. Das liegt an Microsofts AGP-Treiber für VIA-Chipsätze (Viaagp.sys), der mit der Hardware-Änderung nicht zurechtkommt. Benutzer, die VIA-Treiber ihres Mainboard-Herstellers verwenden, sind davon nicht betroffen.

Ein aktualisierter VIA-Treiber von Microsoft ist über den (kostenpflichtigen) Support zu beziehen. Alternativ empfiehlt sich ein Wechsel auf den Herstellertreiber oder der Verzicht auf den Austausch der Grafikkarte, bis der neue Microsoft-Treiber öffentlich verfügbar ist.

Neue AGP-Karte auf Board mit VIA-Chipsatz

Datum	01.07.2002
Betrifft	Windows 2000 (P, S, AS) auf Rechner mit VIA-Board
Wirkung	Nach Installation neuer Grafikkarte hängt das System
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	VIA-Treiber des Mainboard-Herstellers installieren

Infos	Microsoft Knowledgebase

› USB-2.0-Unterstützung

Unterstützung für den 480 Mbit/s schnellen Universal Serial Bus (USB) 2.0 enthält das aktuelle SP3 nicht, es ist jedoch über Windows-Update zu bekommen.

Bis dato kann Windows 2000 aber nur mit den folgenden EHCI-Controllern kommunizieren:

- › NEC PCI to USB Enhanced Host Controller B0 (PCI-ID: PCI\ VEN_1033&DEV_00E0&REV_01)
- › NEC PCI to USB Enhanced Host Controller B1 (PCI-ID: PCI\ VEN_1033&DEV_00E0&REV_02)
- › Intel PCI to USB Enhanced Host Controller (PCI-ID: PCI\ VEN_8086&DEV_24CD)
- › VIA PCI to USB Enhanced Host Controller (PCI-ID: PCI\ VEN_1106&DEV_3104)

USB-2.0-Unterstützung

Datum	19.05.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Keine USB-2.0-Unterstützung
Patch	Über windowsupdate.microsoft.com
Abhilfe	Patch installieren
Infos	Microsoft Knowledgebase

› Kein Zugriff auf EFS

Auf Daten oder Files, die per Systemdienst Protected Storage oder Encrypting Files System (EFS) geschützt werden, kann unter Umständen nach Änderung des Domänen-Passworts nicht mehr zugegriffen werden.

Das liegt daran, dass die Verschlüsselung über einen Hash-Wert des Passworts erfolgt. Bei einer Passwortänderung verschlüsselt Windows 2000 die Daten erst dann neu, wenn das erste Mal darauf zugegriffen wird. Ist nun genau zu diesem Zeitpunkt der Domänen-Controller nicht erreichbar, schlägt die Neuverschlüsselung und damit der Datenzugriff fehl.

Ein Bugfix für dieses Problem ist zwar verfügbar, aber nur über den (kostenpflichtigen) Support zu beziehen. Bis dahin sollten Benutzer, die häufiger nicht mit dem DC verbunden sind, nach einer Änderung des Passworts sofort auf alle geschützten Daten und Files zugreifen. Damit wird die Verschlüsselung an das neue Passwort angepasst.

Kein Zugriff auf EFS

Datum	06.05.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Kein Zugriff auf geschützte Daten
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Nach Änderung des Passworts sofort auf geschützte Daten und EFS zugreifen
Infos	Knowledgebase-Artikel

› Windows bemerkt leere CD-R nicht

Tauscht man eine normale CD-ROM gegen eine unbeschriebene CD-R aus, zeigt der Windows Explorer weiterhin den Inhalt der CD-ROM an. Erst beim Versuch, ein Programm von der CD zu starten, kommt es zur Fehlermeldung.

Es gibt zwar einen Fix von Microsoft, doch dieser ist nur über den (kostenpflichtigen) Support erhältlich.

Windows bemerkt leere CD-R nicht

Datum	10.05.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Explorer zeigt weiterhin Inhalt der vorhergehenden CD an
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Keine
Infos	Microsoft Knowledgebase

› Windows Update erzwingt Scandisk

Wenn der Systemdienst "Automatische Updates" in der Version 3.0 ein kritisches Update auf einem FAT-Systemlaufwerk installiert, kommt es zu folgendem Effekt:

Der Treiber Fastfat.sys setzt beim Neustart des Systems den Status des Dateisystems auf "clean", da alle Daten ordnungsgemäß auf die Platte geschrieben wurden. Als Letztes wird allerdings das Programm Windows Update beendet, das den Status des Dateisystems wieder auf "dirty" setzt. Damit glaubt Windows beim nächsten Systemstart, das Dateisystem sei nicht in Ordnung und meldet, dass der Rechner nicht ordnungsgemäß heruntergefahren wurde. Das könnte bei einem unerfahrenen Anwender zu Irritationen führen.

Einen Patch gibt es derzeit nur beim (kostenpflichtigen) Support. Es reicht allerdings zu wissen, dass mit dem System alles in Ordnung ist.

Windows Update erzwingt Scandisk

Datum	29.05.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Scandisk nach Update
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Ignorieren
Infos	Microsoft Knowledgebase

› CPU-Auslastung 100% bei Notebook-Laden

Bei manchen Notebook-Herstellern ist das Netzteil so schwach ausgelegt, dass die Akkus nur sehr langsam geladen werden, wenn das Gerät gerade benutzt wird. Das an sich ist schon ärgerlich genug, doch unter Windows 2000 kommt noch ein weiterer Effekt hinzu.

Ein Fehler in Cmbatt.sys sorgt dafür, dass die CPU-Last auf 100% steigt, während das Notebook geladen wird. Das Problem ist laut Microsoft der Algorithmus, der den Ladezustand in die Bildschirmanzeige im Systemtray umwandelt.

Ein Patch ist derzeit nur beim kostenpflichtigen Support verfügbar. In der Zwischenzeit empfiehlt es sich für Betroffene, den Rechner während des Ladens nicht zu benutzen.

CPU-Auslastung 100% bei Notebook-Laden

Datum	26.03.2002

Betrifft	Windows 2000 P, S, AS
Wirkung	CPU-Last steigt auf 100%
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Laden nur bei ausgeschaltetem Notebook
Infos	Microsoft Knowledgebase

› Von SP3 behobene Fehler

Um Daten ohne großen Aufwand auszutauschen, bietet sich die Infrarot-Schnittstelle (IrDA) an. Über diese verfügen nicht nur viele Desktops und Notebooks, sondern auch Drucker, PDAs und Handys.

Die Software-seitige Unterstützung ist meist direkt im Betriebssystem integriert. Der in Windows 2000 zuständige IrDA-Treiber enthält jedoch einen ungeprüften Puffer. Speziell manipulierte IrDA-Pakete nutzen diese Lücke und bringen durch einen Pufferüberlauf das angegriffene System zum Absturz.

Pufferüberlauf in IrDA-Treiber

Datum	21.08.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Rechner stürzt ab
Patch	In Deutsch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Speicherleck in NNTP-Dienst

Der NNTP-Dienst, der in NT 4.0, Windows 2000 und Exchange 2000 steckt, enthält ein Speicherleck. Diese Schwachstelle lässt sich mit speziell aufgebauten News-Postings ausnutzen.

Jedes Mal, nachdem die fehlerhafte Routine solch eine manipulierte Nachricht verarbeitet hat, wird der zuvor benötigte Speicher nicht wieder freigegeben. Bei einer entsprechend hohen Zahl manipulierter Anfragen können Angreifer den Server mit einer DoS-Attacke lahm legen.

Speicherleck in NNTP-Dienst

Datum	14.08.2001
Betrifft	NT 4.0; Windows 2000 S, AS; Exchange 2000
Wirkung	DoS-Attacke
Patch	In Deutsch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Manipulierte RPC-Anfragen

Mehrere RPC-Server, von denen Systemdienste in NT 4.0, Windows 2000, SQL- und Exchange-Server abhängen, prüfen Anfragen nicht korrekt. In einigen Fällen werden sogar Angaben akzeptiert, die die normale Verarbeitung verhindern. Die fraglichen Werte variieren von Server zu Server.

Der Schaden, den Hacker über diese Sicherheitslücke verursachen können, hängt vom attackierten RPC-Server und dessen Diensten ab. Die Spanne reicht vom kurzzeitigen "Aussetzer" des Rechners bis zur DoS-Attacke.

Manipulierte RPC-Anfragen

Datum	26.07.2001
Betrifft	Exchange Server 5.5/2000; SQL Server 7.0 / 2000; NT 4.0; Windows 2000 P, S, AS
Wirkung	DoS-Attacke
Patch	In Deutsch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Offenes Mail Relay über SMTP-Dienst

Eine Sicherheitslücke im SMTP-Dienst von Windows 2000 ermöglicht unerwünschtes Mail Relaying. Durch einen Fehler im Authentifizierungsprozess können sich Angreifer mit ungültigen Angaben gegenüber dem Dienst als Benutzer ausweisen. Auf diese Weise lässt sich das System zwar nicht administrieren, aber SMTP nutzen. Was durchaus ausreicht, um den attackierten Rechner als offenes Mail Relay zu verwenden, etwa für Spamming.

Standardmäßig wird der SMTP-Dienst von Windows 2000 nur auf Servern eingerichtet, bei der Professional-Installation muss der Anwender dies explizit angeben.

Offenes Mail Relay über SMTP-Dienst

Datum	05.07.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Unerwünschter Mail Relay
Patch	In Deutsch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Offene Gast-Accounts über FTP-Server finden

Eine Schwachstelle der User-Verwaltung stellt stets der Gast-Account dar: Windows 2000 installiert ihn standardmäßig und ohne Passwort. Zum Glück ist das Gast-Konto per Default nicht aktiviert. Das übernehmen dann - sei es aus Bequemlichkeit oder Unkenntnis - häufig die Administratoren. Ganz Unerfahrene spendieren dabei oft noch ein paar zusätzliche Berechtigungen.

Damit spielen sie einem Angreifer gleich zwei Sachen in die Hände: Einen hinreichend bekannten Account-Namen und ein standardmäßig leeres Passwort. Dieses Szenario auf einem FTP-Server, der Domänenmitglied ist, reißt ein weiteres Sicherheitsloch auf: Stellt jemand beim Einloggen auf diesem Server einem vorhandenen Account statt des Domänennamens eine bestimmte Zeichenfolge voran, sucht der FTP-Dienst in allen angeschlossenen Domänen nach diesem Account. Existiert dort ein offenes Gast-Konto, findet es ein Hacker unter Ausnutzung dieser Lücke garantiert.

Offene Gast-Accounts über FTP-Server finden

Datum	20.06.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Offene Gast-Accounts lassen sich leicht ausfindig machen
Patch	IIS 4.0, IIS 5.0
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Knowledgebase

› Telnet-Dienst - DoS-Attacken

Microsoft stellt einen Patch für den Telnet-Dienst in Windows 2000 bereit, der nicht weniger als sieben Sicherheitslücken schließt. Die Lücken lassen sich einteilen in DoS-Attacken, Erschleichen von Privilegien sowie Aufspüren schlecht administrierter (Gast-)Konten.

Den Telnet-Dienst von Windows 2000 kann ein Hacker auf unterschiedliche Weise für DoS-Attacken missbrauchen. Zum einen ist es möglich, Sitzungen zu starten, die es Telnet unmöglich macht, sie nach Ablauf des Time-Out wieder zu schließen. Bei ausreichender Zahl verstopfen diese offenen Sessions dann den Zugang für andere Benutzer.

Zum anderen lässt sich auch durch wiederholtes Öffnen und Schließen von Sitzungen der Dienst lahm legen. Das Beenden der Sitzungen muss dabei auf eine Weise erfolgen, die Telnet dazu bringt, für die Sitzung verwendete Systemressourcen nicht mehr freizugeben.

Die dritte DoS-Attacke wird über ein Kommando bei der Anmeldung möglich. Telnet stürzt dann ab, und Administratoren müssen den Dienst neu starten, um einen Normalbetrieb zu ermöglichen.

Zu guter Letzt können Angreifer eine Systemfunktion aufrufen und auf diese Weise andere Telnet-Sitzungen schließen. Administratorrechte werden dazu nicht benötigt, normale Zugangsprivilegien reichen vollkommen aus.

General-Patch für Telnet-Dienst

Datum	07.06.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	DoS-Attacken, Ausführen beliebigen Codes sowie Ausspionieren von Benutzernamen
Patch	Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Telnet-Dienst - Privilegienerhöhung und Gastzugang

Für das Erschleichen von Privilegien muss der Angreifer die Rechte besitzen, Programme über Telnet auf den Server zu laden und auszuführen, was eher unwahrscheinlich ist. Gelingt es dem Angreifer aber trotzdem, diese Rechte zu erlangen, kann er die Sicherheitslücke nutzen, um den Server mit allen Rechten zu übernehmen: Telnet vergibt für jede Sitzung eine so genannte Named Pipe. Darin enthaltener Code wird beim Initialisieren der Sitzung ausgeführt. Die mittels Algorithmus vergebenen Namen der Sitzungen lassen sich allerdings leicht vorhersagen. Ein Angreifer kann also eine Named Pipe benennen, die gemäß diesem Namensmuster in nächster Zeit an der Reihe ist, und darin Code seiner Wahl unterbringen. Findet Telnet nach der Namensvergabe eine bereits vorhandene Pipe mit dem Namen, führt der Dienst diese aus.

Das Durchforsten einer oder mehrerer Domänen nach einem bekannten Benutzerkonto gestaltet sich über Telnet ebenso einfach wie über die Lücke in Microsofts FTP-Server. Stellt jemand bei der Telnet-Anmeldung einem vorhandenen Account statt des Domänennamens eine bestimmte Zeichenfolge voran, sucht Telnet in allen angeschlossenen Domänen danach. Besonderer Beliebtheit erfreut sich hierbei der Gastzugang: Er ist hinreichend bekannt und überdies standardmäßig mit leerem Passwort versehen.

General-Patch für Telnetdienst

Datum	07.06.2001

Betrifft	Windows 2000 P, S, AS
Wirkung	DoS-Attacken, Ausführen beliebigen Codes sowie Ausspionieren von Benutzernamen
Patch	Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Ungeprüfter Puffer in Webserver-ISAPI

Über einen ungeprüften Puffer in den ISAPI-Erweiterungen von Microsofts Webserver IIS kann ein Angreifer auf der Zielmaschine beliebigen Code ausführen.

Die Sicherheitslücke tut sich bereits bei der Standardinstallation des IIS auf. Dabei werden mit den ISAPI-Erweiterungen zusätzliche Funktionen ermöglicht. Unter den dafür zuständigen Bibliotheken befindet sich auch die idq.dll, die unter anderem Scripts zur Server-Administration unterstützt. Die Bibliothek ermöglicht zwar auch Suchanfragen des Windows-2000-Indexdienstes (unter NT 4.0: Indexserver aus dem Option Pack), die Lücke öffnet sich jedoch erst durch den IIS.

Dass in der Datei ein ungeprüfter Puffer steckt, hat Microsoft erst relativ spät entdeckt. Daher kommen selbst die Beta-Versionen von Windows XP mit dem Sicherheitsloch.

Mittels Pufferüberlauf ist es einem Angreifer möglich, direkt auf Systemebene mit allen lokalen Rechten zu agieren. Er kann damit etwa Webseiten ändern, Software auf den Server laden oder Letzteren umkonfigurieren.

Ungeprüfter Puffer in Webserver-ISAPI-Erweiterungen

Datum	18.06.2001
Betrifft	Indexserver 2.0 (NT 4.0 Option Pack) und Indexdienst in Windows 2000
Wirkung	Ausführen beliebigen Codes
Patch	Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Missbrauch des BrowserReset Frame

Microsofts Browser-Dienst dient dazu, Netzwerkressourcen zu finden. Durchsucht der Anwender etwa das LAN mit Hilfe des Icons Netzwerkumgebung, unterstützt ihn dabei der Browser-Dienst. Zur Lastverteilung setzt man dabei Master Browser und Backup Browser ein. Master Browser enthalten eine Liste der LAN-Ressourcen und replizieren diese auf die Backup Browser. Die Kommunikation untereinander erfolgt über so genannte Frames.

Über den ResetBrowser-Frame etwa lässt sich der Browser-Dienst beenden. Dies ist beispielsweise hilfreich, wenn eine zu große Browser-Anzahl für eine zu hohe Netzlast durch die entstehende Replikation sorgt.

Da das Protokoll für den Browser-Dienst keine Authentisierung vorsieht, könnte ein Angreifer entsprechende Frames gezielt gegen Rechner einsetzen, um den Anwendern den Zugriff auf Dienste und Computer in einem Netzwerk zu verweigern. Im Extremfall ist auch denkbar, dass auf diesem Weg gefälschte Informationen zur Verfügung gestellt werden.

Missbrauch des BrowserReset Frame

Datum	25.05.2000
Betrifft	Browser-Dienst auf Windows 2000 P, S, AS

Wirkung	ResetBrowser-Frames können für eine Denial-of-Service-Attacke missbraucht werden.
Patch	Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Speicherloch führt zu DoS-Attacken

Über ein Speicherloch bei Windows-2000-Servern ist es möglich, eine DoS-Attacke zu starten. Dazu bombardiert ein Angreifer einen auf Domänen-Controllern laufenden Dienst mit Kerberos-Zertifizierungsanfragen, ohne den entsprechenden Socket auszulesen. Da Windows 2000 den Speicher nicht wieder freigibt, läuft dieser irgendwann über.

Nach etwa 4000 Connect-/Disconnect-Runden, so Peter Gründl von Defcom (http://www.defcom.com) , akzeptiere Kerberos keine Anfragen mehr. Manuell kann man das Speicherproblem nur jeweils durch einen Neustart beheben.

Speicherloch führt zu DoS-Attacken

Datum	08.05.2001
Betrifft	Windows 2000 S, AS
Wirkung	DoS-Attacke durch exzessive Zertifizierungsanfragen
Patch	Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Snap-in für Ereignisanzeige mit ungeprüftem Puffer

Das Snap-in, das die Windows-2000-Ereignisanzeige um zusätzliche Funktionen erweitert, besitzt einen ungeprüften Speicherbereich. Gelingt es, einen manipulierten Eintrag in der Ereignisanzeige unterzubringen, kommt es zu einem Pufferüberlauf.

Dies bewirkt - je nach Art der Manipulation - einen Absturz der Ereignisanzeige oder die Ausführung beliebigen Codes, den ein Angreifer in den ungeschützten Puffer schreibt. Das auf diese Weise eingeschmuggelte Programm würde mit den Berechtigungen desjenigen ausgeführt, der sich den veränderten Eintrag anschaut. Ist das etwa der Administrator, kann es brisant werden.

Abhilfe schafft nur die Installation des Patches.

Snap-in für Ereignisanzeige mit ungeprüftem Puffer

Datum	26.02.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Programmabsturz; Ausführen beliebigen Codes
Patch	Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Network DDE Agent

Network DDE ermöglicht es Applikationen, die auf verschiedenen Rechnern laufen, Daten dynamisch auszutauschen. Das geschieht über Kommunikationskanäle (Trusted Shares), die der Dienst "Network DDE Agent" steuert. Lokale Prozesse richten ihre Anfragen an diesen Dienst, der die Anfragen als Systemkonto verarbeitet.

Ein Angreifer, der manipulierte Anfragen starten kann, hätte dadurch die Möglichkeit, den

Network DDE Agent für seine Zwecke zu benutzen. Er könnte beliebigen Code im Sicherheitskontext des Betriebssystems statt des angemeldeten Users ausführen.

Network DDE Agent

Datum	05.02.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Beliebiger Code kann im Sicherheitskontext des Betriebssystems ausgeführt werden
Patch	Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Snap-In für Active-Directory-User stürzt ab

Mit Windows 2000 hat Microsoft die Active Directory Services (ADS) eingeführt. Mit diesem Verzeichnisdienst lassen sich alle relevanten Netzwerkressourcen, etwa Anwender, Drucker und Server, zentral verwalten.

Den Umgang mit dem Verzeichnisdienst erleichtern Tools, die in der Regel als Snap-In-Module für die Microsoft-Management-Konsole ausgelegt sind. Das Modul zur Verwaltung von Anwendern und Computern weist allerdings einen Bug auf: Markiert man eine "größere Zahl" von Usern, um ihnen über einen rechten Mausklick eine Mail zu schicken, reagiert die Management Console mit einer Zugriffsverletzung.

Snap-In für Active-Directory-User stürzt ab

Datum	02.01.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Eingeschränkte User-Verwaltung über Snap-In für Verzeichnisdienst
Patch	Servicepack 3
Abhilfe	Servicepack 3 installieren
Informationen	Microsoft Knowledgebase

› Terminal Sessions werden gekappt

Clients, die über eine verschlüsselte Session die Terminaldienste eines Windows-2000-Servers nutzen, verlieren immer wieder die Verbindung zum Host. In dessen Systemprotokoll findet sich unter der Ereignis-ID 50 der Hinweis, dass ein Fehler im Protokoll-Stream aufgetreten ist.

Dieser Bug macht sich bemerkbar, wenn im Netzwerk viele fragmentierte IP-Frames auftreten. In dem Fall kann der Server die verschlüsselten Frames der Clients nicht mehr richtig entschlüsseln.

Terminal Sessions werden gekappt

Datum	02.01.2002
Betrifft	Windows 2000 S, AS
Wirkung	Clients verlieren Server-Verbindung
Patch	Servicepack 3
Abhilfe	Servicepack 3 installieren
Informationen	Microsoft Knowledgebase

› Speicherleck durch ungültige Checksummen

Auf Windows-2000-Rechnern mit aktivierten Terminaldiensten kann es zu einem Speicherleck beim nicht ausgelagerten Kernel-Speicher kommen. Dies führt zu empfindlichen Einschränkungen des Netzwerkverkehrs, da auf Client-Anfragen keine Antwort mehr erfolgt oder nur noch stark verzögert.

Verantwortlich dafür zeigt sich ein Bug im Treiber tdtcp.sys. Der Treiber kann mit IP-Paketen, die ungültige TCP-Checksummen aufweisen, nicht richtig umgehen.

Mittlerweile hat Microsoft einen Patch bereitgestellt.

Speicherleck durch ungültige Checksummen

Datum	20.06.2001
Betrifft	Windows 2000 S, AS
Wirkung	Störungen des Netzwerkverkehrs
Patch	Auf Deutsch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Knowledgebase

› Exzessive CPU-Last durch ungültige Anfragen

Ein Bug in einem auf allen Domänen -Controllern aktiven Dienst unter Windows 2000 kann zu einer DoS-Attacke führen. Dieser Dienst verwirft ungültige Serviceanfragen eines bestimmten Typs nicht unmittelbar, sondern beginnt mit einer ressourcenintensiven Verarbeitung und sendet erst danach eine Antwort.

Eine Überflutung mit solchen Anfragen treibt die CPU-Belastung des Domänen-Controllers derart hoch, dass User sich nicht mehr anmelden können. Für bereits eingeloggte Anwender verlangsamt sich der Zugriff auf Netzwerkressourcen spürbar. Hat der Administrator aufgepasst, blockiert eine Firewall den Zugriff von außen auf die dabei benutzten Ports - Sabotageakte von innen lassen sich damit aber nicht abfangen.

Exzessive CPU-Last durch ungültige Anfragen

Datum	20.02.2001
Betrifft	Windows 2000 S, AS
Wirkung	Denial-of-Service-Attacke gegen Domänen-Controller
Patch	In Deutsch
Abhilfe	Patch oder Servicepack 3 installieren
Informationen	Microsoft Security Bulletin

› Zyklischer Neustart von Domänen-Controllern

Auf einem oder mehreren Domänen-Controllern in einer Windows-2000-Domäne erscheint die Fehlermeldung, dass der Systemprozess LSASS.EXE mit dem Statuscode -1073741571 beendet wurde und der Rechner nun neu startet. Dieses Verhalten wiederholt sich zirka alle 15 Minuten.

Verantwortlich für das abrupte Beenden von LSASS.EXE ist ein Stack-Überlauf in der Konsistenzprüfung, die die Datenreplikation im Netzwerk dynamisch anpasst. Ab einer bestimmten Anzahl von Active-Directory-Replikationsobjekten tritt der Fehler auf.

Zyklischer Neustart von Domänen-Controllern

Datum	21.04.2001

Betrifft	Windows 2000 S, AS
Wirkung	Zyklischer Neustart von Domänen-Controllern
Patch	Servicepack 3
Abhilfe	Servicepack 3 installieren
Informationen	Microsoft Knowledgebase

› Eigenschaften-Menü lässt sich nicht ausblenden

In größeren IT-Umgebungen, speziell im Firmenumfeld, achten Administratoren auf eine annähernd einheitliche Installation. Damit das auch so bleibt, lassen sich Richtlinien (Policies) definieren, die den Anwendern eine bestimmte Arbeitsumgebung vorgeben. In den Policies ist etwa geregelt, welche Desktop-Komponenten oder Menüpunkte ausgeblendet werden.

Wer allerdings das Eigenschaften-Menü der Icons "Arbeitsplatz" oder "Eigene Dateien" sperren möchte, wird dazu keine Möglichkeit entdecken. Das gelingt erst, wenn man einen entsprechenden Patch installiert, den es aber nur auf Anfrage bei Microsoft gibt. Außerdem muss man nach der Installation die Registry editieren.

Dazu trägt man unter HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ Explorer Folgendes ein:

- › Wertename: NoPropertiesMyComputer
- › Typ: DWORD
- › Basis: Dezimal
- › Wert: 1
- › Wertename: NoPropertiesMyDocuments
- › Typ: DWORD
- › Basis: Dezimal
- › Wert: 1

Um die Umgebung nicht nur für den aktuell angemeldeten, sondern für alle Benutzer zu ändern, wählt man statt HKEY_CURRENT_USER den Zweig unter HKEY_LOCAL_MACHINE.

Eigenschaften-Menü lässt sich nicht ausblenden

Datum	06.01.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Benutzer können die Eigenschaften von "Arbeitsplatz" und "Eigene Dateien" aufrufen
Patch	Servicepack 3
Abhilfe	Servicepack 3 installieren und Registry anpassen
Informationen	Microsoft Knowledgebase

› Nach Service Pack 2 keine Server-Dienste

Administratoren, die auf ihren Windows-2000-Servern Service Pack 2 (SP2) installieren, sperren damit einige User aus. Typischerweise trifft es diejenigen, die sich mit einem Client unter Win 9x/Me über ein VPN einwählen: In dieser Konstellation lassen sich Datei- und Druckdienste des Servers oder Exchange nicht mehr nutzen. Das Phänomen taucht ebenfalls bei Clients auf, die unter NT 4.0 oder Windows 2000 laufen, wenn andere als Microsoft-VPN-Server eingesetzt werden oder Router mit NAT.

Die Kommunikationsprobleme zwischen Client und Server entstehen, weil beide sich

nicht auf eine gemeinsame Größe der Netzwerkpakete einigen können. Server mit SP2 ignorieren ICMP-Nachrichten, die sie dazu auffordern, eine kleinere MTU zu verwenden.

Nach Service Pack 2 keine Server-Dienste

Datum	02.01.2002
Betrifft	Windows 2000 P, S, AS
Wirkung	Clients können Server-Dienste nicht mehr nutzen
Patch	Servicepack 3
Abhilfe	Servicepack 3 installieren
Informationen	Microsoft Knowledgebase

› Windows Installer und CD-ROMs

Software, die die Windows-Installer-Technologie nutzt, bereitet unter bestimmten Bedingungen Ärger. Das passiert etwa immer dann, wenn das Setup Dateien aus einem CAB-Archiv auf der CD-ROM extrahieren will. Ignoriert der Anwender die wenig aussagekräftige Fehlermeldung "Interner Fehler 2351" oder "Interner Fehler 2355", ist die Chance hoch, dass anschließend die installierte Software nicht richtig funktioniert.

Wer nicht das Servicepack 2 aufspielen möchte, muss sich mit ein paar Vorschlägen zum Workaround zufrieden geben. So empfiehlt Microsoft, vor dem Starten der Installationsroutine Windows mit so wenig Treibern wie möglich hochzufahren, am besten im abgesicherten Modus. Hilft das nicht, sollte man die Dateien von der CD in einen Ordner auf der Festplatte kopieren und von dort das Setup aufrufen. Als letzte Möglichkeit geben die Techniker aus Redmond den Tipp, ein anderes CD-ROM-Laufwerk auszuprobieren.

Windows Installer und CD-ROM-Installation

Datum	02.06.2001
Betrifft	Windows 9x, NT 4.0, Windows 2000 P, S, AS
Wirkung	Software mit Windows-Installer-Technologie lässt sich nicht richtig installieren
Patch	Servicepack 2
Abhilfe	Servicepack 2 installieren
Informationen	Microsoft Knowledgebase

› Fehlerhaftes Internet Printing Protocol

Windows 2000 unterstützt mit dem Internet Printing Protocol (IPP) einen Industriestandard, der dazu dient, Druckjobs mittels HTTP zu übergeben und zu steuern. Die Implementierung in das Betriebssystem hat Microsoft über eine ISAPI-Erweiterung realisiert, die Windows 2000 standardmäßig installiert. Auf sie zugreifen kann man aber nur über den IIS 5.0.

Allerdings haben die Programmierer in Redmond bei der Implementierung vergessen, einen für Eingabeparameter vorgesehenen Speicherbereich abzufragen. Entsprechend manipulierte Anfragen führen daher zu einem Pufferüberlauf, der den Angreifer in die Lage versetzt, beliebige Programme auszuführen. Diese laufen im Sicherheitskontext des Systemkontos und ermöglichen so die komplette Kontrolle des angegriffenen Systems. Damit die Attacke gelingt, muss lediglich Port 80 (HTTP) oder 443 (HTTPS) offen sein.

Fehlerhafte Implementierung des Internet Printing Protocol

Datum	01.05.2001
Betrifft	Windows 2000 P, S, AS

Wirkung	Angreifer kann beliebigen Code ausführen
Patch	Servicepack 2 oder Windows 2000 Security Patch
Abhilfe	Patch installieren
Informationen	Microsoft Security Bulletin

› Druckjobs ab 4 MByte

Umfangreiche Druckjobs, die größer als 4 MByte sind, werden entweder überhaupt nicht oder nur unvollständig gedruckt.

Das GDI verwendet einen fehlerhaften Algorithmus zur Bestimmung der in Zeilen angeordneten Rasterdaten, den so genannten *scan lines*. Beim Rendering des Druckjobs entsteht daher eine Differenz zwischen der vorab (falsch) berechneten und der tatsächlichen Zeilenzahl. In diesem Fall geht das GDI davon aus, dass der Druckjob korrumpiert ist und löscht ihn.

Als Workaround bietet es sich an, umfangreiche Druckjobs zu verkleinern, indem man beispielsweise große Dokumente aufteilt. Die kritische Grenze, ab der der Fehler auftritt, lässt sich nur durch Trial and Error herausfinden.

Druckjobs ab 4 MByte

Datum	18.04.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Große Druckjobs ab 4 MByte werden nicht oder nur teilweise gedruckt
Patch	Servicepack 2
Abhilfe	Servicepack 2 installieren. Alternativer Workaround: Aufteilung von großen Druckjobs
Informationen	Microsoft Knowledgebase

› Anmeldung in gemischter Umgebung

Gerade große Unternehmen mit einigen tausend Rechnern steigen nicht auf einen Schlag auf ein neues Betriebssystem um. Dies gilt in besonderem Maße für die Migration von Servern.

Hat der Administrator nun zunächst einen Domänen-Controller auf Windows 2000 umgestellt, versuchen sich alle Windows-2000-Clients ausschließlich an diesem Rechner anzumelden. Während der migrierte Server unter der Last der Authentifizierungsanfragen ächzt, liegen die NT-Anmeldeserver brach.

In der Microsoft Knowledgebase fand sich dazu vor kurzem noch der lapidare Hinweis, dies stelle ein standardmäßiges Verhalten dar. Mittlerweile spricht der Software-Hersteller von einem "Problem", das Servicepack 2 beseitigt.

Anmeldung in gemischter Umgebung (NT 4.0/Windows 2000)

Datum	17.04.2001
Betrifft	Windows 2000 S, AS
Wirkung	Windows-2000-Clients melden sich in gemischter Umgebung nur an Windows-2000-Servern an
Patch	Servicepack 2
Abhilfe	Servicepack 2 installieren
Informationen	Microsoft Knowledgebase

› Kein ATA-100

Kein Bug per se, aber Windows 2000 unterstützt derzeit kein ATA-100 (http://www.tecchannel.de/hardware/453/index.html) (Mode 5) für Festplatten. ATA-100-Festplatten steuert Windows 2000 mit ATA-66 an. Ein entsprechendes Update stand vor Servicepack 2 zwar schon zur Verfügung, allerdings nur auf Anfrage.

Ob sich der (kostenpflichtige) Anruf beim Microsoft-Support für den separaten Patch gelohnt hat, ist fraglich. Denn die meisten Festplatten schaffen die Datenrate ohnehin nicht. Mehr über ATA-100-Festplatten lesen Sie in unserem aktuellen Festplatten-Vergleich (http://www.tecchannel.de/hardware/498/) .

Kein ATA-100

Datum	27.07.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Windows 2000 steuert ATA-100-Platten als ATA-66 an
Patch	Servicepack 2
Abhilfe	Servicepack 2 installieren
Informationen	Microsoft-Knowledgebase

› SUBST-Laufwerke sind persistent

Mit Hilfe des noch aus DOS-Zeiten stammenden Befehls SUBST können böswillige Mitarbeiter Benutzern, die sich später einloggen, ein beliebiges Laufwerk unterschieben. Beispielsweise erzeugt der Befehl *» subst m: d:\temp ein «* das Laufwerk M. Liegt dort normalerweise das Home-Verzeichnis, schreibt der nächste Benutzer seine Daten nicht in das Home-Verzeichnis, auf das er allein Zugriff hat, sondern nach d:\ temp, auf das jeder Benutzer Zugriff hat.

Ein durch SUBST erzeugtes Laufwerk wird nämlich beim Log-off nicht entfernt, das heißt, es bleibt bestehen. Somit kann es passieren, dass der nächste Benutzer seine Dateien beispielsweise nicht auf dem Netzwerklaufwerk speichert, sondern auf einem lokalen, das der vorherige Benutzer per SUBST erzeugt hat.

Hier gibt es zwar einen Patch, dieser ist jedoch nur auf Anfrage beim (kostenpflichtigen) Support zu erhalten. Um das beschriebene Problem zu lösen, können Sie die Datei subst.exe aus dem Verzeichnis system32 von Windows 2000 löschen oder umbenennen.

SUBST-Laufwerke sind persistent

Datum	02.01.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Ein böswilliger Nutzer kann dem nächsten, der sich anmeldet, ein beliebiges Laufwerk unterschieben
Patch	Servicepack 2
Abhilfe	Servicepack 2 installieren. Als Workaround kann man subst.exe löschen oder umbenennen
Informationen	Microsoft Knowledgebase

› Administrator hat keinen Zugriff auf Profile

Beim Erstellen eines Server-basierten Profils vergibt Windows 2000 lediglich Zugriffsrechte für das System und den Benutzer, nicht jedoch für den Administrator. Damit hat er auch keinen Zugriff auf diesen Ordner.

Das Verhalten mag zwar hinsichtlich des Datenschutzes wünschenswert sein, erschwert dem Administrator allerdings die Arbeit. Für Änderungen müsste er zunächst den Besitz

über diesen Ordner übernehmen und sich dann die entsprechenden Rechte zuteilen. Daher sollte der Administrator vor dem Einrichten des Server-basierten Profils das entsprechende Verzeichnis von Hand anlegen und die Rechte vergeben.

Administrator hat keinen Zugriff auf Profile

Datum	15.11.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Administrator kann Server-basierte Profile nicht bearbeiten
Patch	Servicepack 2
Abhilfe	Servicepack 2 installieren oder Verzeichnis für Profil von Hand anlegen
Informationen	Microsoft Knowledgebase

› Fragmentierte Registry verhindert Start

Wenn die Registry von Windows 2000 zu fragmentiert ist, bleibt das System beim Start hängen, weil der Bootloader mit der Fragmentierung nicht klarkommt. Da der mitgelieferte Diskeeper nur als Light-Version vorliegt und die Auslagerungs- und Registry-Dateien nicht berücksichtigt, hilft auch das Defragmentieren des Bootlaufwerks nicht. Dieser Bug betrifft nur Systeme, bei denen Windows 2000 auf einem NTFS-Laufwerk installiert ist. Partitionen unter FAT und FAT32 sind nicht betroffen. Ein entsprechender Patch ist nur auf Anfrage beim (kostenpflichtigen) Support zu erhalten.

Sie haben zwei Möglichkeiten, dieses Problem zu beheben.

1.) Wenn Ihr System bereits betroffen ist, starten Sie Windows 2000 unter der Recovery-Konsole und geben nacheinander die folgenden Befehle ein:

» *cd \winnt\system32\config*
» *rename system system.org*
» *copy system.org system*
» *exit*

2.) Ist Ihr System noch nicht betroffen, können Sie ein Auftreten des Bugs mit der Installation von Servicepack 2 oder mit dem Utility PageDefrag aus unserer Utilities für Windows NT/2000 (http://www.tecchannel.de/betriebssysteme/215/4.html) -Sammlung verhindern.

Fragmentierte Registry verhindert Start

Datum	15.11.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Wenn die Registry auf einem NTFS-Laufwerk liegt und zu stark fragmentiert ist, startet Windows 2000 nicht mehr
Patch	Servicepack 2
Abhilfe	Servicepack 2 installieren oder vorbeugend Registry regelmäßig defragmentieren
Informationen	Microsoft Knowledgebase

› Zugriff auf NTFS-Wechselmedien

Wenn ein Benutzer ohne Administrator-Rechte unter NTFS ein Wechselmedium formatiert, kann er später nicht auf dieses Medium zugreifen. Das liegt daran, dass Windows 2000 die ACL des Mediums nicht korrekt anpasst, weil der formatierende Benutzer keine ausreichenden Rechte hat, um die ACL zu erzeugen.

Als Abhilfe formatieren Sie Wechselmedien nur unter dem Administrator-Account oder

spielen den Patch von Microsoft ein.

Zugriff auf NTFS-Wechselmedien

Datum	15.11.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Benutzer können auf NTFS-Wechselmedien nicht zugreifen.
Patch	Servicepack 2 oder separater Patch
Abhilfe	Patch oder Servicepack einspielen
Informationen	Microsoft-Knowledgebase

› DNS-Cache lässt sich nicht löschen

In bestimmten Situationen kann es erforderlich sein, den Cache eines Servers zu löschen, etwa weil sich darin ungültige Daten befinden. Versucht der Administrator, den Cache eines DNS-Servers unter Windows 2000 zu löschen, erhält er eine Fehlermeldung.

Microsoft stellt einen Patch nur auf Anfrage zur Verfügung.

DNS-Cache lässt sich nicht löschen

Datum	02.05.2000
Betrifft	DNS-Dienst in Windows 2000 S, AS
Wirkung	Der Cache des DNS-Servers lässt sich nicht löschen
Patch	Servicepack 2
Abhilfe	Servicepack 2 installieren
Informationen	Microsoft Knowledgebase

› Gefälschte VeriSign-Zertifikate

VeriSign (http://www.verisign.com/) hat Ende Januar 2001 zwei auf "Microsoft Corporation" ausgestellte digitale Class-3-Zertifikate an einen vermeintlichen Microsoft-Angestellten ausgegeben (http://www.tecchannel.de/news/20010323/thema20010323-3979.html) . Wer den zur Authentifizierung von ausführbaren Programmen beim Download vorgesehenen Zertifikaten vertraut, öffnet Angreifern Tür und Tor.

Die VeriSign-Zertifikate lassen sich benutzen, um Programme, ActiveX-Controls, Office-Makros und ähnlichen ausführbaren Code zu signieren. Vor allem ActiveX und Makros stellen eine besondere Gefahr dar, warnt Microsoft.

Das Update enthält eine Liste zurückgezogener Schlüssel, in der die fraglichen Zertifikate als ungültig aufgeführt sind. Alternativ sollten Benutzer die Annahme von Zertifikaten verweigern, die das Datum des 29. oder 30. Januar 2001 tragen. An diesen Tagen wurden die falschen Digital-IDs ausgegeben. Dagegen wurden an keinem der beiden Tage Zertifikate für Microsoft selbst ausgestellt.

Datum	22.03.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Angriffe durch vermeintlich von Microsoft signierte Programme
Patch	Servicepack 2 oder Windows Security Patch
Abhilfe	Patch oder Servicepack installieren
Informationen	Microsoft Security Bulletin

› Service Control Manager

Der Service Control Manager von Windows 2000 ist das zentrale Instrument, über das die Systemdienste erzeugt oder modifiziert werden. Für jeden Systemdienst legt der SCM eine so genannte Named Pipe mit einem speziellen Namen an. Wenn nun ein Programm genau diese Named Pipe erzeugt, bevor der SCM dies tun kann, erhält das Programm die Privilegien des Systemdienstes.

Service Control Manager

Datum	1.08.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Ein Programm kann sich die Privilegien eines Systemdienstes aneignen und entsprechend viel Unheil anrichten
Patch	Servicepack 2 oder Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack installieren
Informationen	Microsoft Security Bulletin

› Relative Shell Path

Der Registry-Eintrag, der auf den Windows Explorer verweist, arbeitet mit relativen Pfadnamen statt mit absoluten. Dieser relative Pfadname kann jedoch beim Systemstart noch nicht aufgelöst werden, daher durchsucht die Bootroutine das Systemlaufwerk nach der Datei *explorer.exe*. Dabei wird zuerst das Root-Verzeichnis durchsucht. Platziert nun ein böswilliger Benutzer dort eine Datei namens *explorer.exe*, wird beim nächsten Systemstart dieses Programm als Shell verwendet statt des richtigen Windows Explorer.

Relative Shell Path

Datum	28.07.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Ein böswilliger Nutzer kann dem nächsten, der sich anmeldet, ein beliebiges Programm als Shell unterschieben.
Patch	Servicepack 2 oder Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack installieren
Informationen	Microsoft Security Bulletin

› SNMP-Sicherheit

Die Registry-Schlüssel für die SNMP-Konfiguration von Windows 2000 sind nicht genügend abgesichert, so dass ein Hacker diese Einträge verändern und danach über SNMP den betroffenen Rechner angreifen kann. Es sind nur Rechner betroffen, auf denen der SNMP-Dienst installiert wurde.

Das von Microsoft bereitgestellte Sicherheits-Update passt die fehlerhaften Registry-Rechte an. Spielen Sie entweder das Servicepack 2 oder den separaten Patch ein. Falls Sie den SNMP-Dienst nicht benötigen, können Sie ihn auch über die Systemsteuerung deinstallieren.

SNMP-Sicherheit

Datum	22.12.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Ein Hacker kann zunächst die Registry verändern und

	danach über SNMP den Rechner angreifen
Patch	Servicepack 2 oder Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack installieren
Informationen	Microsoft Security Bulletin

› Sysmon mit ungeprüftem Puffer

Im Sysmon-ActiveX-Control von Windows 2000 hat Microsoft einen ungeprüften Pufferspeicher eingebaut, den Hacker dazu nutzen können, beliebigen Programmcode auf einem Rechner zu starten. Da ActiveX-Controls auch über den IE oder Outlook zu starten sind, bietet sich Hackern über eine Website oder E-Mails eine gute Angriffsfläche.

Generell sollten Sie die Sicherheitseinstellungen im IE so hoch setzen, dass ActiveX-Controls nicht einfach so ausgeführt werden können. In Outlook sollten Sie ActiveX komplett untersagen.

Sysmon mit ungeprüftem Puffer

Datum	28.07.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Hacker können beliebigen Programmcode auf einem angegriffenen Rechner ausführen
Patch	Servicepack 2 oder Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack installieren
Informationen	Microsoft Security Bulletin

› NetBIOS Nameserver Spoofing

Das NetBIOS Nameserver (NBNS) Protocol ist in der WINS-Implementation von Windows eingebunden. Es enthält einige Funktionen, um Namenskonflikte aufzulösen (etwa wenn zwei Arbeitsrechner denselben Namen tragen). Über spezielle Protokollaufrufe können Arbeitsrechner auch in die Auflösung von Namenskonflikten eingreifen. Diese Aufrufe kann ein Hacker ausnutzen, um etwa dem Rechner "WORK2" mitzuteilen, dass er ab jetzt "WORK15" heißt. Der reguläre WINS-Server weiß davon nichts und somit ist die betroffene Arbeitsstation nicht mehr über den Namen "WORK2" zu erreichen.

Dieser Bug kann auch von einem Hacker im Internet ausgenutzt werden, wenn der Port 137 für UDP-Pakete geöffnet ist.

Auch wenn ein Patch zur Verfügung steht, sollten dennoch in Netzwerken, die mit dem Internet verbunden sind, an der Firewall die Ports 137 bis 139 geblockt werden. Damit kann zumindest kein Hacker von außen das Netzwerk negativ beeinflussen.

NetBIOS Nameserver Spoofing

Datum	27.07.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Ein Hacker kann bestimmte Arbeitsstationen blocken, indem er ihnen einen anderen Namen zuweist
Patch	Servicepack 2 oder Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack installieren
Informationen	Microsoft Security Bulletin

› IP Fragment Reassembly

IP-Pakete, die die maximale Frame-Größe in einem Netzwerk überschreiten, gelangen als Fragmente aufgesplittet an ihr Ziel. Dort muss sie das Betriebssystem in der richtigen Reihenfolge zusammensetzen und weiter verarbeiten.

Befinden sich ungültige Daten in den fragmentierten IP-Paketen, treibt dies die Arbeitslast auf dem Zielrechner drastisch nach oben. Der angegriffene Computer ist beinahe ausschließlich mit der Bearbeitung der kompromittierenden Fragmente beschäftigt. Im Extremfall kann er dabei abstürzen.

IP Fragment Reassembly

Datum	19.05.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Ungültige Daten in IP-Fragmenten lassen sich für eine Denial-of-Service-Attacke missbrauchen
Patch	Servicepack 1 oder Windows 2000 Security Patch
Abhilfe	Patch oder Servicepack installieren
Informationen	Microsoft Security Bulletin

› NNTP kann Hash-Tabelle nicht neu erzeugen

Wenn der NNTP-Dienst die Hash-Tabelle neu aufbaut, bringt ihn eine Nullnachricht ins Schleudern. Als Folge bricht er den Vorgang ab, anstatt die Nachricht als ungültig zu markieren und fortzufahren. Damit ist die Hash-Tabelle nicht vollständig und nicht zu nutzen.

Das Problem ist im Servicepack 1 behoben.

NNTP kann Hash-Tabelle nicht neu erzeugen

Datum	10.03.2000
Betrifft	NNTP-Dienst in Windows 2000 P, S, AS
Wirkung	Die Hash-Tabelle wird bei einer ungültigen Nachricht nicht neu aufgebaut
Patch	Servicepack 1
Abhilfe	SP1 installieren
Informationen	Microsoft Knowledgebase

Speicherloch im NNTP-Dienst

Beim Löschen abgelaufener Nachrichten verbraucht der NNTP-Dienst Hauptspeicher, der nicht automatisch wieder freigegeben wird. Dadurch muss Windows 2000 mehr virtuellen Speicher bereitstellen, der die System-Performance drückt.

Speicherloch im NNTP-Dienst

Datum	10.03.2000
Betrifft	NNTP-Dienst in Windows 2000 P, S, AS
Wirkung	Ein Speicherloch im NNTP-Dienst verbraucht immer mehr Speicher, der erst bei einem Neustart des Rechners wieder freigegeben wird
Patch	Servicepack 1
Abhilfe	SP1 installieren oder regelmäßige Neustarts
Informationen	Microsoft Knowledgebase

› Stabilitätsprobleme - IIS

Viele Administratoren verlassen sich auf den Internet Information Server, weil er bei Windows NT/2000 dabei ist und für die meisten Aufgaben durchaus genügt. Allerdings sollten Administratoren gerade bei einem so sensiblen Thema wie Webservern immer aufmerksam die Bugreports zum IIS verfolgen.

Internet Information Server stürzt ab

Der IIS 5.0 reagiert auf bestimmte Zeichen im HTTP-Request-Header mit einer Schutzverletzung. Er wird zwar von Windows 2000 automatisch neu gestartet, doch Hacker können dieses Problem für eine DoS-Attacke missbrauchen, indem sie den IIS ständig abstürzen lassen.

Wer IIS 5.0 als Webserver einsetzt, sollte sich den Servicepack 1 holen.

Internet Information Server stürzt ab

Datum	14.03.2000
Betrifft	IIS 5.0 von Windows 2000
Wirkung	Bei bestimmten Zeichen im HTTP-Header stürzt der IIS ab
Patch	Servicepack 1
Abhilfe	SP1 installieren
Informationen	Microsoft Knowledgebase

IIS findet Dateien nicht mehr

Bestimmte Dateierweiterungen wie etwa .htm lassen sich über die Funktion "App Mappings" im Internet Service Manager von IIS so markieren, dass sie über das Include Statement andere Dateien einschließen können. Verwendet jedoch ein Default-Dokument, wie beispielsweise index.htm, ein Include Statement, kommt es zur Fehlermeldung "401 Zugriff verweigert" beim Internet-Nutzer. Das Problem tritt nicht auf, wenn der Dokumentenname dezidiert angegeben wird, also beispielsweise www.server.de/index.htm.

Das Problem ist in Servicepack 1 behoben.

IIS findet Dateien nicht mehr

Datum	15.02.2000
Betrifft	IIS 5 und Windows 2000 P, S, AS
Wirkung	Default-Dokumente mit Include Statements werden nicht mehr angezeigt.
Patch	Servicepack 1
Abhilfe	SP1 installieren
Informationen	Microsoft Knowledgebase

› Global Catalog Server schießt Windows ab

Über den Aufruf der Funktion sbTableGetDSName mit einem leeren Parameter in LegacyExchangeDN lässt sich der Global Catalog Service von Windows 2000 mit einem Bluescreen abschießen.

Der Global Catalog enthält Informationen über alle Domains im Verzeichnis. Über ihn können Benutzer und Anwendungen Objekte im gesamten Active Directory suchen. Die enthaltenen Informationen beschränken sich auf die wichtigsten Suchbegriffe (wie etwa

Nachname oder Username) und Links auf die Originalobjekte in den einzelnen Domains.

Global Catalog Server schießt Windows ab

Datum	10.03.2000
Betrifft	Global Catalog Service in Windows 2000 S, AS
Wirkung	Über einen ungültigen Parameter lässt sich ein Bluescreen hervorrufen
Patch	In Servicepack 1
Abhilfe	SP1 installieren
Informationen	Microsoft Knowledgebase

› Datenausspähung per Index-Server

Der Indexdienst von Windows 2000 indiziert HTML-, Word-, Excel- und PowerPoint-Dokumente und stellt über den Internet Information Server eine Suchmaschine zur Verfügung. Die so genannte Hit-Highlighting-Funktion enthält jedoch einen Fehler, über den Webbenutzer auch Zugriff auf Dokumente erhalten können, die nicht im Internet-Verzeichnis liegen und dementsprechend nicht veröffentlicht werden sollen. Um Zugriff zu erhalten, muss der Internet-Benutzer lediglich den Pfad- und Dateinamen angeben. Der Index-Server liefert dann die Textstelle mit dem gefundenen Schlüsselwort.

Der ursprüngliche, im Microsoft Security Bulletin MS00-006 (http://www.microsoft.com/technet/security/bulletin/MS00-006.asp) erwähnte Patch bewirkt nichts gegen eine neue Variante der Sicherheitslücke. Diese ermöglicht es, weitere Dateitypen auszuspähen. Erst der nach dem Servicepack 2 herausgebrachte Einzel-Patch sorgt für Abhilfe.

Datenausspähung per Index-Server

Datum	10.05.2001
Betrifft	Indexdienst in Windows 2000 P, S, AS und Index-Server 2.0 in NT 4.0
Wirkung	Es lassen sich auch Dokumente abrufen, die eigentlich nicht für den Webzugriff gedacht sind
Patch	Windows Security Patch
Abhilfe	Patch installieren
Informationen	Microsoft Security Bulletin

› Speicherloch im DNS-Dienst

Der Domain Name Service (DNS) ist im Internet der Standard zur Auflösung von Server-Namen in IP-Adressen. Eine Anfrage nach www.tecChannel.de etwa wandelt ein DNS-Server in die zugehörige IP-Adresse um.

In Windows 2000 hat Microsoft den DNS-Dienst um so genannte Service-Einträge ergänzt. Mit deren Hilfe lassen sich so wichtige Informationen ermitteln wie der für die Anmeldung notwendige Domänen-Controller.

Für jede Anfrage allokiert der DNS-Dienst Speicher, den er jedoch nicht wieder automatisch freigibt. Dadurch wächst die Systembelastung, da Windows 2000 mehr virtuellen Speicher bereitstellen muss.

Dieser Fehler ist in Servicepack 1 behoben.

Speicherloch im DNS-Dienst

Datum	10.04.2000

Betrifft	DNS-Dienst in Windows 2000 S, AS
Wirkung	Ein Speicherloch im DNS-Dienst verbraucht immer mehr Speicher, der erst bei einem Neustart des Rechners wieder freigegeben wird
Patch	Servicepack 1
Abhilfe	SP1 installieren oder regelmäßige Neustarts
Informationen	Microsoft Knowledgebase

› Keine Trennung bei FTP-Timeout

Wer regelmäßig Daten per FTPübertragt, stößt früher oder später auf die Meldung, dass der FTP-Server keine weiteren Verbindungen erlaubt, da die maximale Anzahl an Nutzern erschöpft ist. Diese Obergrenze gleichzeitig möglicher Sessions soll eine Mindest-Performance des Servers gewährleisten.

Damit inaktive Clients nicht permanent Ressourcen belegen, lässt sich Server-seitig ein Timeout-Wert einstellen, nach dessen Ablauf die Verbindung getrennt wird.

Ein Fehler im FTP-Dienst von Windows 2000 ignoriert diese Vorgabe jedoch, so dass die maximale Anzahl an Verbindungen schneller erreicht und neue Sessions blockiert werden.

Dieser Fehler ist in Servicepack 1 behoben.

Keine Trennung bei FTP-Timeout

Datum	30.04.2000
Betrifft	FTP-Dienst in Windows 2000 S, AS
Wirkung	Windows 2000 ignoriert den Timeout-Wert für inaktive FTP-Clients
Patch	Servicepack 1
Abhilfe	SP1 installieren
Informationen	Microsoft Knowledgebase

› SMTP-Server ausgebremst

Der SMTP-Server von Windows 2000 bremst sich selbst aus, wenn eine Vielzahl von derzeit unzustellbaren Mails im Ausgang liegt. Diese unzustellbaren Mails blockieren Filehandles, so dass für andere Mails unnötig viele Dateioperationen ausgeführt werden müssen. Diese Operationen kosten Rechenzeit und verlangsamen das System.

Microsoft hat einen Patch für dieses Problem erstellt. Damit stellt der SMTP-Server Mails, die wegen Unerreichbarkeit des Ziel-Servers nicht ausgeliefert werden können, zunächst zurück und verwendet die Filehandles für die Verarbeitung anderer Nachrichten.

SMTP-Server ausgebremst

Datum	13.03.2000
Betrifft	SMTP-Server von Windows 2000 AS
Wirkung	Bei einer großen Menge unzustellbarer Mails kommt es zu Performance-Einbußen
Patch	Servicepack 1
Abhilfe	SP1 installieren
Informationen	Microsoft Knowledgebase

› Netzwerkprobleme

Unter Netzwerkproblemen sind alle Bugs zusammengefasst, die Windows 2000 im Netzwerkbetrieb betreffen.

Benutzer kann Passwort nicht ändern

Wenn ein NT-Server auf Windows 2000 Active Directory aufgerüstet und danach bei einem Benutzer die Option "Benutzer kann Passwort nicht ändern" zurückgesetzt wird, kann er sein Passwort trotzdem nicht ändern. Windows 2000 entfernt zwar den ACE (Access Control Entry), der den Schreibzugriff auf das Passwort verhindert, es setzt aber nicht den zusätzlich notwendigen ACE, der das Schreiben explizit erlaubt.

Eine Übergangslösung ist das manuelle Setzen des entsprechenden ACE in der Management Console unter "Active Directory Benutzer und Computer".

Benutzer kann Passwort nicht ändern

Datum	08.03.2000
Betrifft	Active Directory von Windows 2000 S, AS
Wirkung	Benutzer können nach einem Upgrade des Servers auf Windows 2000 ihr Passwort nicht ändern.
Patch	Servicepack 1
Abhilfe	SP1 installieren oder manuelle Änderung der ACE
Informationen	Microsoft Knowledgebase

Probleme mit Server-basierten Profilen

Wenn ein Server-basiertes Profil auf einem Share gespeichert ist, das auch Services für Macintosh anbietet, kann es beim Log-in zu einer Fehlermeldung kommen. Windows beschwert sich, dass bestimmte Dateien nicht vom Share kopiert werden können und darum das Profil ungültig ist. Als Folge weist Windows dem Benutzer ein temporäres Profil zu, das beim Ausloggen wieder gelöscht wird.

Probleme mit Server-basierten Profilen

Datum	14.02.2000
Betrifft	Windows 2000 S, AS
Wirkung	Server-basierte Profile sind nicht verfügbar
Patch	Servicepack 1
Abhilfe	SP1 installieren oder Server-basierte Profile nicht auf Shares anlegen, die für Macintosh-Dienste vorgesehen sind.
Informationen	Microsoft Knowledgebase

› Probleme bei Anwendungen

Windows 20000 wird nicht nur als Server eingesetzt, sondern ebenso auf Arbeitsstationen. Daher ist es auch wichtig, dass Applikationen problemlos funktionieren. Alle Applikationen verwenden API-Funktionen des Betriebssystems, so dass ein Fehler in der API auch die Applikation beeinträchtigt.

Framemaker kann nicht als PDF speichern

Auf Grund eines Fehlers in der DLL für Postscript-Funktionen (pscript5.dll) erhalten Framemaker-Anwender beim Versuch, ein Dokument als PDF oder als Separationsdatei zu speichern, einen Fehler.

Um die volle Funktionalität von Framemaker wieder herzustellen, sollten Sie den von

Microsoft bereitgestellten aktuellen Patch downloaden. Die erste Version des Patches konnte wegen einer fehlenden digitalen Signatur nicht auf den Rechner aufgespielt werden.

Framemaker kann nicht als PDF speichern

Datum	15.03.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Framemaker kann Dokumente nicht als PDF- oder als Separationsdatei speichern
Patch	auf Deutsch oder Servicepack 1
Abhilfe	SP1 installieren oder Patch einspielen
Informationen	Microsoft Knowledgebase

Assertion-Meldung bei Gif-Bildern

Bei manchen Programmen, die Gif-Bilder über die OLE-Bibliotheken verarbeiten, kann sich das Programm bei bestimmten Bildern mit einer Assertion-Meldung verabschieden. Dabei handelt es sich um Debug-Code, der eigentlich in der Release-Version nicht mehr enthalten sein sollte.

Das Problem ist mit dem Critical Update vom 17. Februar 2000 behoben.

Assertion-Meldung bei Gif-Bildern

Datum	15.02.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Grafikprogramme verabschieden sich bei manchen Gif-Bildern mit einer Assertion-Meldung
Patch	Auf Deutsch oder Servicepack 1
Abhilfe	SP1 installieren oder Patch einspielen
Informationen	Microsoft Knowledgebase

› Probleme mit Iomega-Laufwerken

Die Wechsellaufwerke von Iomega (http://www.iomega.com/) erfreuen sich auch im professionellen Umfeld großer Beliebtheit, weil sie den Datenaustausch zwischen Rechnern vereinfachen. Allerdings gibt es gerade bei den Modellen für den Parallelport einige Probleme.

Zip-Software findet Laufwerk nicht

Die Zip-Tools finden auf einem Rechner mit Windows 2000 ein an den Parallelport angeschlossenes Zip- oder Jaz-Laufwerk nicht. Der Grund ist, dass die Zip-Tools SCSI-Kommandos senden, und Windows 2000 SCSI-Kommandos an Parallelports nicht unterstützt.

Mit einem Update der Parallelport-Treiber können die Zip-Tools wieder auf die Laufwerke zugreifen.

Zip-Software findet Laufwerk nicht

Datum	19.02.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Zip-Tools finden Laufwerke nicht am Parallelport
Patch	Auf Deutsch oder Servicepack 1
Abhilfe	SP1 installieren oder Patch einspielen

Informationen	Microsoft Knowledgebase

Iomega Jaz funktioniert nicht

Das Jaz-Laufwerk von Iomega funktioniert nicht, wenn es per Jaz Traveller (Adapter SCSI auf Parallel) an den PC angeschlossen ist und nicht auf SCSI-ID 5 oder 6 eingestellt ist. Microsoft hat noch keinen offiziellen Patch für dieses Problem. Bis dahin sollte das Laufwerk einfach auf ID 5 oder 6 eingestellt werden.

Iomega Jaz funktioniert nicht

Datum	18.02.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Iomega Jaz wird erkannt, kann aber nicht angesprochen werden
Patch	Servicepack 1
Abhilfe	SP1 installieren oder SCSI-ID auf 5 oder 6 einstellen
Informationen	Microsoft Knowledgebase

› Allgemeine Probleme

In dieser Rubrik finden sich Probleme, die in keine der anderen Kategorien passen oder keine schwer wiegende Funktionsbeeinträchtigung darstellen.

Fremde Kerberos-Realms unerwünscht

Wird ein Kerberos-Server, der nicht unter Windows 2000 läuft, zu der Realm-Liste von Windows 2000 hinzugefügt, tritt die Änderung erst nach einem Neustart von Windows 2000 in Kraft.

Ein Patch steht mittlerweile zur Verfügung. Administratoren müssen also Windows 2000 nicht immer wieder starten, sobald ein neuer Kerberos-Server zur Realm-Liste hinzugefügt wird.

Fremde Kerberos-Realms unerwünscht

Datum	08.05.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Neuer Kerberos-Server wird nicht automatisch eingebunden
Patch	Windows 2000 Patch oder Servicepack 1
Abhilfe	SP1 installieren oder Patch einspielen
Informationen	Microsoft Knowledgebase

Hartnäckige Lautstärkekontrolle

Wenn Windows 2000 per Suspend schlafen geschickt wird, taucht beim Neustart die Lautstärkekontrolle in der Task-Leiste auf, auch wenn sie vorher ausgeschaltet war.

Dieser optische Störenfried hat keinen Einfluss auf die Funktionsfähigkeit von Windows 2000. Daher lohnt es sich auch nicht, den Patch (kostenpflichtig) vom Microsoft-Support zu ordern. Im nächsten Servicepack ist er garantiert behoben.

Hartnäckige Lautstärkekontrolle

Datum	14.03.2000

Betrifft	Windows 2000 P, S, AS
Wirkung	Lautstärkekontrolle taucht nach Resume in der Task-Leiste auf
Patch	Servicepack 1
Abhilfe	SP1 installieren
Informationen	Microsoft Knowledgebase

Fehler in xenroll.dll

In der deutschen Version von Windows 2000 ist Microsoft ein Fehler unterlaufen, der den Austausch von Sicherheitszertifikaten unmöglich macht. Die dafür zuständige DLL xenroll.dll ist nicht digital signiert, so dass die Gegenstelle sich weigert, Sicherheitszertifikate auszutauschen.

Der entsprechende Patch ist auf der Microsoft-Website verfügbar und sollte installiert werden, wenn der beschriebene Fehler auftritt. Ansonsten können Anwender bis zum ersten Servicepack von Windows 2000 abwarten.

Fehler in xenroll.dll

Datum	02.03.2000
Betrifft	Windows 2000 P, S, AS
Wirkung	Probleme beim Austausch von Sicherheitszertifikaten
Patch	In Deutsch oder Servicepack 1
Abhilfe	SP1 installieren oder Patch einspielen
Informationen	Microsoft Knowledgebase

› NetWare-Login-Script erzeugt Fehler

Um Rechner an Novell-Server anzubinden, steckt im Windows-Paket der Client Service für NetWare. Dessen Script-Prozessor Nwscript.exe interpretiert die NetWare-Login-Scripts. Das gelingt bei NetWare 4.x allerdings nicht fehlerfrei: Nwscript.exe erzeugt eine Zugriffsverletzung an Adresse 0x01cae84b.

Häufigste Fehlerursache ist laut Microsoft die Verwendung von Else-Anweisungen im Script, wenn Sie anschließend ein DOS-Programm aufrufen. Der empfohlene Workaround aus Redmond lautet lapidar: Vermeiden Sie Else-Anweisungen, wenn dadurch DOS-Kommandos ausgeführt werden. Wer auf solche Konstrukte nicht verzichten kann, sollte vielleicht die Treiber von Novell selbst ausprobieren. Sie befinden sich auf dem Support-Server (http://support.novell.de) unter "Product Downloads".

NetWare-Login-Script erzeugt Fehler

Datum	09.08.2001
Betrifft	Windows NT 4.0; Windows 2000 P, S, AS
Wirkung	NetWare-Login-Script wird nicht abgearbeitet
Patch	Nicht verfügbar
Abhilfe	Verzicht auf Else-Statements mit anschließendem DOS-Befehl; NetWare-Client von Novell einsetzen
Informationen	Microsoft Knowledgebase

› Neu: Pufferüberlauf durch manipulierte SMB-Pakete

Windows verwendet das SMB-Protokoll, damit Clients auf Ressourcen wie Dateien, Drucker oder Schnittstellen im Netzwerk zugreifen können. Schickt ein Client ein

SMB-Paket, das eine kleinere Puffergröße angibt als erforderlich wäre, an den Server, sollte der Server die Diskrepanz bemerken und das Paket verwerfen.

Doch ein Fehler bei der Gültigkeitsprüfung führt zu einem Pufferüberlauf. Auf diese Weise kann ein Angreifer ein System zum Absturz bringen, Daten zerstören oder beliebigen Code ausführen.

Servicepack 4 stopft die Sicherheitslücke.

Pufferüberlauf durch manipulierte SMB-Pakete

Datum	09.07.2003
Betrifft	NT (Terminal-) Server 4.0; Windows 2000 P, S, AS; Windows XP Professional
Wirkung	Ausführen beliebigen Codes
Patch	Servicepack 4
Abhilfe	Servicepack 4 installieren
Informationen	Microsoft Knowledgebase und Security Bulletin

› Neu: Abstürze durch NetBIOS-Treiber

Wer auf die NetBIOS-Unterstützung in Windows 2000 angewiesen ist, muss mit periodisch auftretenden Abstürzen leben. Ein Bug im Treiber Netbt.sys verursacht die Fehlermeldung STOP 0x000000C2 BAD_POOL_CALLER, ausgelöst durch Anfragen auf falschem IRQ-Level oder eine ungültige Speicheroperation.

Ein entsprechender Patch ist nur auf Anfrage beim (kostenpflichtigen) Support zu erhalten.

Abstürze durch NetBIOS-Treiber

Datum	24.06.2003
Betrifft	Windows 2000 P, S, AS
Wirkung	Computer hängt sich auf
Patch	Nur auf Anfrage bei Microsoft
Abhilfe	Patch installieren
Informationen	Microsoft Knowledgebase

› Neu: Blockierte GDI-Threads

Unter Deadlock versteht man einen Zustand, bei dem sich zwei oder mehr Prozesse gegenseitig blockieren. Wenn nicht wenigstens ein Prozess den Konflikt erkennt, führt das zum Einfrieren des Systems.

Exakt diese Pattsituation kann auftreten, wenn Programme mit Hilfe der Funktion EnableEUDC versuchen, ein benutzerdefiniertes Zeichen zu erstellen oder zu speichern. Ergebnis: Der Rechner reagiert nicht mehr.

Das Problem lässt sich mit einem Hotfix von Microsoft beseitigen.

Blockierte GDI-Threads

Datum	28.05.2003
Betrifft	Windows 2000 P, S, AS
Wirkung	Computer hängt sich auf
Patch	auf Deutsch ((http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=ABE71533-E
Abhilfe	Patch installieren

Informationen	Microsoft Knowledgebase

› Neu: Zugriffsverletzung bei Anmeldung

Gleich beim ersten Anmelden begrüßt Windows User mit einer Zugriffsverletzung in der Datei Unregmp2.exe. Dieser Fehler betrifft ausschließlich Anwender ohne Administratorrechte und tritt nur einmal auf. Trotzdem bleibt ein ungutes Gefühl - schließlich weiß niemand, welche Nebenwirkungen dadurch eventuell noch auftreten.

Servicepack 4 behebt den Bug.

Zugriffsverletzung bei Anmeldung

Datum	26.06.2003
Betrifft	Windows 2000 P, S, AS
Wirkung	Erstmaliges Anmelden ohne Administratorrechte verursacht Fehlermeldung
Patch	Servicepack 4
Abhilfe	Servicepack 4 installieren
Informationen	Microsoft Knowledgebase

› Neu: Sicherheitslücke in DirectX

DirectX, Bestandteil aller modernen Windows-Versionen, ist von einer gravierenden Sicherheitslücke betroffen. Zwei Buffer Overruns in der DirectX-Komponente DirectShow erlauben es Angreifern, über manipulierte MIDI-Dateien beliebigen Code auf dem betroffenen Rechner auszuführen.

Windows-2000-User, die das Servicepack 4 installiert haben, sind auf der sicheren Seite.

Sicherheitslücke in DirectX

Datum	23.07.2003
Betrifft	Alle Windows-Varianten mit DirectX-Versionen von 5.2 bis 9.0a
Wirkung	Ausführen beliebigen Codes
Patch	Servicepack 4
Abhilfe	Servicepack 4 installieren
Informationen	Microsoft Knowledgebase und Security Bulletin

› Neu: Sicherheitsleck im Utility Manager

Die in Windows integrierten Eingabehilfen, mit denen sich die Funktionen für Behinderte steuern lassen, weisen eine Schwachstelle auf. Der so genannte Utility Manager prüft Windows-Messages nur unzureichend, was ein Angreifer dazu missbrauchen kann, über speziell formatierten Programmcode beliebige Aktionen auf dem System auszuführen. Voraussetzung: Der Unbefugte hat sich an der lokalen Konsole oder über den Terminal-Manager angemeldet.

Servicepack 4 behebt den Fehler.

Sicherheitsleck im Utility Manager

Datum	09.07.2003
Betrifft	Windows 2000 P, S
Wirkung	Ausführen beliebigen Codes

Patch	Servicepack 4
Abhilfe	Servicepack 4 installieren
Informationen	Microsoft Knowledgebase und Security Bulletin

› Drucken über lokalen oder Gast-Account

Druckt ein Anwender über einen lokalen oder Gast-Account auf einen Netzwerkdrucker, landet der Druckjob zwar in der Queue des Printservers, wird aber nicht abgearbeitet. Im Systemprotokoll des Servers findet sich stattdessen ein Eintrag mit der Event-ID 45.

Kurios: Meldet sich ein Administrator an dem Printserver an und druckt eine Testseite, tritt das Phänomen bei nachfolgenden Druckaufträgen nicht mehr auf. Das gilt allerdings nur so lange, bis der Printserver neu gestartet wird.

Drucken über lokalen oder Gast-Account

Datum	20.06.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Druckjob wird nicht abgearbeitet
Patch	Nur auf Anfrage
Abhilfe	Keine
Informationen	Microsoft Knowledgebase

› Servicepack 2 erscheint nicht mehr unter Installieren/Deinstallieren

Hat der Anwender sich beim Update auf Servicepack 2 für das Backup der bestehenden Dateien entschieden, lässt sich später der Fix wieder deinstallieren. Der entsprechende Eintrag unter Software im Dialogfeld Installieren/Deinstallieren der Systemsteuerung verschwindet jedoch beim Upgrade von Internet Explorer 5.5 auf die Version 6.0.

Installiert man dann noch einmal Servicepack 2, diesmal ohne die vom Setup angebotene Backup-Option, sucht man die Deinstallationsmöglichkeit für den Internet Explorer 6 in der Systemsteuerung vergeblich.

Microsoft rät in diesem Fall zu einem so genannten "In-Place-Upgrade". Dazu legt man die Original-Windows-2000-CD ein und weist das Setup an, die bestehende Installation zu "aktualisieren". Anschließend installiert man den Internet Explorer und dann das Servicepack 2 - in dieser Reihenfolge.

Servicepack 2 erscheint nicht mehr unter Installieren/Deinstallieren

Datum	02.06.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Es existiert kein Eintrag mehr, um Servicepack 2 zu deinstallieren
Patch	Nicht verfügbar
Abhilfe	Workaround durch In-Place-Upgrade
Informationen	Microsoft Knowledgebase

› Falsche Verzeichnisinhalte

Verbindet man sich zu einem Share auf einem Server, können in einigen freigegebenen Verzeichnissen Dateien angezeigt werden, die auf einem anderen Share liegen. Das Problem tritt nur über das Netzwerk auf und betrifft ausschließlich Freigaben auf NTFS-Partitionen.

Voraussetzungen für diesen Fehler: Es gibt viele Freigaben mit ähnlichen

Verzeichnisstrukturen, und die Hauptverzeichnisse der Shares tragen kurze ähnliche Namen. Die über die ACLs festgelegten Dateiberechtigungen werden dadurch jedoch nicht ausgehebelt.

Ursache des Fehlverhaltens: Unter bestimmten Bedingungen verweist NTFS beim Zugriff auf Verzeichnisinhalte auf eine Tabelle, die keinerlei Bezug zu den Inhalten der freigegebenen Verzeichnisse hat.

Microsoft stellt einen Patch nur auf Anfrage zur Verfügung.

Falsche Verzeichnisinhalte

Datum	27.04.2001
Betrifft	Windows 2000 P, S, AS
Wirkung	Anzeige falscher Verzeichnisinhalte
Patch	Nur auf Anfrage
Abhilfe	Keine
Informationen	Microsoft Knowledgebase

› Neu: Keine Treiberinstallation über die Seite Windows Update

Microsoft bietet über die Seite Windows Update (http://windowsupdate.microsoft.com) nicht nur Hotfixes für Sicherheitslücken an, sondern auch aktualisierte Treiber. Deren Installation scheitert jedoch, falls sich im Windows-Unterverzeichnis Inf "eine große Anzahl" von Inf-Dateien befindet. Eine genauere Mengenangabe bleibt Microsoft schuldig.

Das Problem lässt sich mit Servicepack 4 beheben.

Keine Treiberinstallation über die Seite Windows Update

Datum	05.06.2003
Betrifft	Windows 2000 P, S, AS; Windows XP Home/Professional/Media Center/Tablet PC
Wirkung	Treiber von der Seite Windows Update lassen sich nicht installieren
Patch	Servicepack 4
Abhilfe	Servicepack 4 installieren
Informationen	Microsoft Knowledgebase

› Neu: Festplatten-Performance nimmt ab

Besonders ärgerlich für Administratoren: Die Festplatten-Performance der von ihnen betreuten Systeme sinkt kontinuierlich. Nur durch einen Neustart der Rechner lässt sich die gewohnte Leistung wieder herstellen.

Eine starke Fragmentierung der Festplatte scheidet damit als Grund aus. Verursacher ist vielmehr der Classpnp-Treiber. Er überwacht Datenträger, um festzustellen, ob sie unter zu hoher Last stehen. Die damit einhergehende erhöhte Fehlerzahl veranlasst den Treiber, zunehmend Leistungsfunktionen der Datenträger zu deaktivieren. Das dynamische Reaktivieren dieser Funktionen unterstützt er indes nicht.

Servicepack 4 schafft Abhilfe.

Festplatten-Performance nimmt ab

Datum	26.06.2003
Betrifft	Windows 2000 P, S, AS
Wirkung	Festplatte wird spürbar langsamer
Patch	Servicepack 4

Abhilfe	Servicepack 4 installieren
Informationen	Microsoft Knowledgebase

› Weitere Themen zu diesem Artikel:

Windows XP Bugreport (http://www.tecchannel.de/betriebssysteme/818/index.html)
Windows NT Bugreport (http://www.tecchannel.de/betriebssysteme/172/index.html)
Windows Me Bugreport (http://www.tecchannel.de/betriebssysteme/610/index.html)
Windows 98 Bugreport (http://www.tecchannel.de/betriebssysteme/79/index.html)
Internet-Explorer-Sicherheitslücken (http://www.tecchannel.de/internet/185/index.html)
Sicherheitslücken im Netscape Communicator (http://www.tecchannel.de/internet/63/index.html)
Office-97-Bugreport (http://www.tecchannel.de/software/84/index.html)
Office-2000-Bugreport (http://www.tecchannel.de/software/302/index.html)
Windows 2000: Zum Spielen geeignet (http://www.tecchannel.de/betriebssysteme/245/index.html)
Windows-2000-Benchmarks (http://www.tecchannel.de/betriebssysteme/247/index.html)
Windows 2000: Treiber/USB-Report (http://www.tecchannel.de/betriebssysteme/249/index.html)